EXPOSING THE eCRIME ECOSYSTEM
Using Threat Intelligence to get ahead of Ransomware attacks

JASON RIVERA, DIRECTOR: STRATEGIC THREAT ADVISORY GROUP, GLOBAL
JASON RIVERA
DIRECTOR: STRATEGIC THREAT ADVISORY GROUP, GLOBAL

• **14+ years**: Innovating at the intersection of security operations & technology

• **U.S. Government**: Former Intelligence Officer/Captain in the U.S. Army; assignments with National Security Agency (NSA), U.S. Cyber Command (USCYBERCOM); served in combat tours overseas

• **Private Sector**: Built threat intelligence & cybersecurity programs for large Fortune 500 companies and U.S. government agencies

• **Education**: M.A. – Security Studies from Georgetown University; M.A. – Economics from the University Of Oklahoma; B.A. – Political Science & Economics from University of Nevada – Las Vegas

• **Thought Leadership**: Black Hat, RSA Conference, Gartner Conference, NATO Conference On Cyber Conflict; InfoSecWorld Conference & Expo
HOW WE COLLECT INTELLIGENCE
THREAT INTELLIGENCE FOCAL POINTS

ADVERSARY & TECHNICAL INTELLIGENCE

DIGITAL RISK MONITORING
UNPRECEDENTED ENDPOINT VISIBILITY & INTELLIGENCE COLLECTION

- TENS OF MILLIONS of endpoints
- 180+ COUNTRIES
- 4+ TRILLION events per week
- 3.4+ BILLION malware samples
- 1.2+ MILLION malware collected daily
- UNENCRYPTED attack telemetry data
MULTI-FACETED INTELLIGENCE COLLECTION APPARATUS

TENS OF MILLIONS OF ENDPOINTS

180+ COUNTRIES

4+ TRILLION EVENTS PER WEEK

3.4+ BILLION MALWARE SAMPLES

1.2+ MILLION MALWARE COLLECTED DAILY

UNENCRYPTED ATTACK TELEMETRY DATA

ENDPOINT TELEMETRY

INCIDENT RESPONSE

MALWARE & FORENSICS

NETWORK TELEMETRY

UNDERGROUND COMMUNITIES

OPEN SOURCE (OSINT)

HIGH FIDELITY

LOW FIDELITY

TLP AMBER
DIGITAL RISK MONITORING COLLECTION SOURCES

- **OPEN WEB**
  - BLOGS, GITHUB, PASTEBIN, ETC

- **SOCIAL MEDIA**
  - TWITTER, REDDIT, DISCORD, ETC

- **MESSAGING APPS**
  - TELEGRAM, QQ, IRC, ETC

- **CRIMINAL FORUMS**
  - BLACKHAT, RAID, EXPLOIT, XSS, ETC

- **CRIMINAL MARKETS**
  - JOKERS STASH, GENESIS, ETC

- **ADVERSARY INFRASTRUCTURE**
  - C2, BOTNETS, DDOS, ETC

- **8+ BILLION**
  - OBJECTS COLLECTED

- **1+ MILLION**
  - UNIQUE SOURCES

- **500+ MILLION**
  - DAILY SOCIAL MEDIA POSTS

- **55+ THOUSAND**
  - UNIQUE DARK WEB SITES

- **8+ YEARS**
  - HISTORICAL DATA

- **42+ MILLION**
  - INDICATORS OF COMPROMISE
AGENDA

UNDERSTANDING THE RANSOMWARE ECOSYSTEM

SERVICES

DISTRIBUTION

MONETIZATION

THE WAY FORWARD
UNDERSTANDING
THE RANSOMWARE ECOSYSTEM
The eCrime ecosystem is an active and diffuse economy of financially motivated entities who engage in myriad criminal activities in order to generate revenue.

The market dynamics as observed by the CrowdStrike Intelligence team over the past several years are fluid; as new mechanisms and schemes are devised to generate revenue, new avenues of monetization are identified, and the global geopolitical and economic landscape changes as adversaries evolve their tactics to maximize profits. This underground economy parallels the global markets in many ways. In order to understand the ebbs and flows of this ecosystem, CrowdStrike has devised a computed value we are dubbing the eCrime Index (ECX) to assess the state of eCrime. The index is based on various observables, weighted by impact, that are continuously monitored by our subject matter experts. The ECX helps identify notable changes that can then be further investigated. We will share analysis results of such events on this site.
UNDERSTANDING THE CRIMINAL ECOSYSTEM

SERVICES
Capabilities that enable eCrime activity

DISTRIBUTION
The vehicles through which capabilities are delivered to victims

MONETIZATION
The methods leveraged to capitalize on successful capability execution against victims
THE CRIMINAL ECOSYSTEM

1 Services

- Access briers
- Phishing kits
- Ransomware
- Malware/giving services
- Webinject kits
- Credits/debit card testing services
- Loaders
- Malware hosting & infrastructure
- Counter anti-virus service/ checkers
- Recruiting for criminal groups

2 Distribution

- SQLi attack tools
- Anonymity and encryption
- Crime-as-a-Service
- eCrime enabling capabilities

- Social network and instant message spam
- Exploit kit development
- Spam email distribution
- Purchasing traffic and/or traffic distribution systems (TDS)

3 Monetization

- Methods to capitalize on successfully executed capabilities

Vehicles delivering capabilities to victims

- Money laundering
- Money transfer
- Money laundering & extortion
- Cash for cards
- Barter payments & extortion
- Counterfeiting
- Wire fraud
- Dump shops
- Collection and resale of payment card information
SERVICES
THE CRIMINAL ECOSYSTEM

1 Services
- Access brokers
- Phishing kits
- Credit/debit card testing services
- Malware packing services
- Webinject kits
- Adversary-controlled services
- Hosting & infrastructure
- Recruitling for criminal groups

2 Distribution
- Social network and instant message spam
- Exploit kit development
- Spam email distribution
- Purchasing traffic and/or traffic distribution systems (TDS)

Vehicles delivering capabilities to victims

3 Monetization
- Methods to capitalize on successfully executed capabilities
- Dump shops
- Collection and liquidation of payment card information
- Money laundering
- Barter payments & extortion

eCrime enabling capabilities
- DDoS attack tools
- Anonymity and encryption
- Spammers
- Loaders
- Counter-anti-virus service/ checkers
Access Brokers
WHAT

- Common tactic that occurs when criminals use real credentials to commandeer an account and perform fraudulent transactions

SO WHAT?

- Step 1: Initial infection
- Step 2: Cred harvesting & device configuration collection
- Step 3: Bot herder assembly
- Step 4: Underground marketplace monetization
- Step 5: Secondary intrusion

WHAT NEXT

- Focus on pre-exploitation prevention and awareness
WHAT
- Prolific Access Broker
- Sells access across the globe
- Focus on government, oil & gas, and technology

SO WHAT?
- Partnered with THANOS developer
- Provided each other positive reviews, increasing reputation in top level Russian language forum
- Indicates growing contacts and capabilities
WHAT?
• Since 13 January 2021, CrowdStrike Intelligence has observed an actor advertising a new private, invitation-only automated shop in a Russian-language forum and in a private communications channel. The shop offers hidden remote desktop protocol (HRDP) access to active victim machines.

SO WHAT?
• The shop utilizes bots—synonymous with connections to victim machines—to establish the HRDP connections to victim machines. Users of the shop are required to purchase access to a bot before they are able to access the associated victim machine. Once access is purchased, a user can access the victim machine at their discretion. Access to bots is shared among all users who have paid for the specific bot.

• HRDP allows access to unique IPs, device fingerprints, saved cookies, and passwords on the victim machine, and it allows the actor to operate under the victim’s user profile.
Access Broker Uses ManageEngine Vulnerability to Obtain Access

**WHAT?**
- CrowdStrike intelligence observed an actor selling access to the remote monitoring and management (RMM) software used by companies. This provides the following access and abilities:
  - File transfer
  - CMD on all systems with NT authority/system privileges
  - Deploy files on all systems
  - Run files on all systems
  - Uninstall antivirus (AV) on systems
  - Monitor processes
  - Access to domain controller, file server, and some backup devices

**SO WHAT?**
- The actor has posted domain administrator access to a U.S.-based food and beverage company, a health services company, a U.S.-based manufacturing company, an oil company, agricultural company, U.S.-based financial company, a Europe-based manufacturing company, a Portugal-based investment company, and many others.
Ransomware
WHAT
MAZE ransomware: first observed MAY 2019
▪ TWISTED SPIDER best known for data extortion
  ▪ Pioneered Complex anti-analysis techniques
  ▪ Used with various banking trojans
  ▪ Hosts data leaks from other ransomware operations

SO WHAT?
▪ TWISTED SPIDERS ability to pioneer new technique has inspired others to use similar capabilities within their own variants

WHAT NEXT?
▪ Follow updates to Maze via Intel reporting
▪ Obtain all associated IOCs
▪ Obtain updated YARA rules
▪ Engage in Threat Hunting

Threat Actor: TWISTED SPIDER
▪ Last Known Activity: February 2021
▪ Community Identifiers: Maze Team, Egregor
▪ Origins: Eastern Europe, Russia

Data Extortion:
1. Recon
2. Ransom
3. Extortion
4. Data Leak
CARBON SPIDER PROVIDES DARKSIDE 2.0 DEVELOPMENT UPDATE

“So What?”
• CARBON SPIDER initially advertised Darkside 2.0 on 9 March 2021 and has issued multiple updates for the ransomware since its release. According to the post, CARBON SPIDER has developed an automated “calling system”, likely referring to phone calls. The adversary is planning to develop a PowerShell version of Darkside 2.0, as well as a “great update for Linux”.

“What?”
• On 24 March 2021, CrowdStrike Intelligence observed a post on a criminal forum that provided an update on CARBON SPIDER’s development of version 2.0 of the Darkside Ransomware-as-a-Service (RaaS).

“What Next?”
• Engage in Campaign Tracking against this threat actor in order to assess evolutions in TTPs, malware, and other capabilities.

<table>
<thead>
<tr>
<th>Malware Name</th>
<th>First Used</th>
<th>Threat Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domenus Stager</td>
<td>July 2020</td>
<td>Stager</td>
</tr>
<tr>
<td>Domenus VBS</td>
<td>April 2020</td>
<td>Downloader</td>
</tr>
<tr>
<td>Domensus JS</td>
<td>September 2020</td>
<td>Downloader</td>
</tr>
<tr>
<td>KillACK</td>
<td>June 2020</td>
<td>Backdoor</td>
</tr>
<tr>
<td>Harpy</td>
<td>May 2018</td>
<td>Backdoor</td>
</tr>
<tr>
<td>Sekur</td>
<td>Summer 2015</td>
<td>RAT</td>
</tr>
<tr>
<td>Darkside</td>
<td>August 2020</td>
<td>Ransomware</td>
</tr>
</tbody>
</table>
DARKSIDE RANSOM DEMANDS CORRELATE WITH VICTIM REVENUE
RANSOMWARE-AS-A-SERVICE PAYMENT PROCESS WORKFLOW

SUCCESSFUL OPERATION ➔ RANSOM COLLECTION ➔ CONTROLLER PAYMENT ➔ CONTROLLER VALIDATION ➔ OPERATOR PAYMENT
PINCHY SPIDER RELEASES VERSION 2.04 OF THE REvil RANSOMWARE

Threat Actor: PINCHY SPIDER
• Last Known Activity: March 2021
• Community Identifiers: GandCrab; REvil; Sodinokibi; GOLD GARDEN; GOLD SOUTHFIELD
• Origins: Eastern Europe, Russia

“What?”
• CrowdStrike Intelligence observed the distribution of PINCHY SPIDER’s REvil ransomware version 2.04. The following changes have been observed since version 2.03 of the REvil ransomware:
  • Safe mode (-smode) command-line parameter with RunOnce persistence
  • Asynchronous Windows Management Interface (WMI) process and service enumeration for termination
  • Change to version of Google Chrome user-agent used in command-and-control (C2) communications

“So What?”
• The continued evolution of REvil’s capabilities combined with the proliferation potential of the ransomware-as-a-service (RaaS) business model increases PINCHY SPIDER’s ability to engage in BGH style attacks against enterprises throughout the world.
THE CRIMINAL ECOSYSTEM

1 Services
- Access brokers
- Phishing kits
- Pespamware
- Malware-purchasing services
- Webinject kits
- Hardware for sale
- Loaders
- Counterfeit antivirus service/checkers
- Hosting & infrastructure
- Recruiting for criminal groups

2 Distribution
- Social network and instant message spam
- Exploit kit development
- Spam email distribution
- Purchasing traffic and/or traffic distribution systems (TDS)
- Vehicles delivering capabilities to victims

3 Monetization
- Methods to capitalize on successfully executed capabilities
- Dump shops
- Collection and sale of payment card information
- Wire fraud
- Money laundering
- Barter for services
- Anonymous mix networks

eCrime enabling capabilities
WHAT
▪ Adversaries are spoofing authority figures in order to increase the credibility and effectiveness of their attacks

SO WHAT?
▪ These messages will also contain elements to inspire a sense of urgency to increase the chance of engagement

WHAT NEXT?
What is your counter-phishing strategy?
• Awareness
• Analyze phishing messages
• Response if there is an interaction
WHAT

- Operations in 2020 relied on LinkedIn personas to engage individuals of interest.
- Personas were disguised as HR, recruiters or sales associates with job opportunities

SO WHAT?

- Following initial contact, communications move to encrypted messaging applications
- In these applications, a malicious file is delivered that retrieves and executes malware
- Malicious files are often disguised as job descriptions, interview request, or trojanized applications
Threat Actor: MALLARD SPIDER

- Last Known Activity: April 2021
- Community Identifiers: Qakbot, QBot, Quakbot, PinkSlip
- Origins: Eastern Europe, Russia
- Target Industries: Aerospace, Finance, Health, Hospitality, Manufacturing, Pharma, Tech, Telecom, Transportation

“What?”
- Qakbot (a.k.a. Qbot) is a sophisticated banking trojan operated by the eCrime actor MALLARD SPIDER. This adversary has been operating one of the longest-running active cybercriminal operations and was first observed in mid-2009.

“So What?”
- Qakbot is a malware family uniquely attributed to and operated by MALLARD SPIDER. Qakbot is able to steal emails, user credentials, and deploy additional malware.
- Qakbot utilizes a modular design to extend its core functionality.
- In December 2020, MALLARD SPIDER made fundamental changes to the architecture of Qakbot, making it more difficult to detect.
- The network communication protocol changed from a URL encoding format to a JSON format.
- The malware configuration is now stored within the Windows registry; in the previous version of the malware, the configuration was stored in an encrypted file.

**Qakbot Default Form Grabber Capture Filter Examples**

<table>
<thead>
<tr>
<th>URL Capture Filter</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>tdetreasury.tdbank.com</td>
<td>tssportal.jpmorgan.com</td>
</tr>
<tr>
<td>cmoltp.bbt.com</td>
<td>ktt.key.com</td>
</tr>
<tr>
<td>cashmanageronline.bbt.com</td>
<td>onlineserv/CM</td>
</tr>
<tr>
<td>.hsbcnet.com</td>
<td>premierview.membersunited.org</td>
</tr>
<tr>
<td>.ebc.ebc</td>
<td>directline4biz.com</td>
</tr>
<tr>
<td>.bilk.com</td>
<td>.webcashmgmt.com</td>
</tr>
<tr>
<td>.bankfct.com</td>
<td>tmconnectweb</td>
</tr>
<tr>
<td>.cmol.bbt.com</td>
<td>moneymanagergps.com</td>
</tr>
<tr>
<td>securetrycorp.zionsbank.com</td>
<td>ibc.klikbc.com</td>
</tr>
<tr>
<td>tmcb.zionsbank.com</td>
<td>directpay.wellsfargo.com</td>
</tr>
<tr>
<td>.web-access.com</td>
<td>express.53.com</td>
</tr>
</tbody>
</table>
**Operational Example**

**Step 1:**
- Select Botnet family: Qakbot.

**Step 2:**
- Search for Botnet family: Qakbot.

**Step 3:**
- View hit details:
  - **Botnet Family:** Qakbot
  - **Type:** Inject
  - **SHA256:** f794b5712a5d5cd00bb95c469fc414fd0e514a0d0f7d9b64f23cd1b1262b57b2
  - **Targets:**
    - Pattern: https://www...
MONETIZATION
THE CRIMINAL ECOSYSTEM

1 Services
- Access brokers
- Phishing kits
- Crypto mining services
- Malware/packaging services
- Webinject kits
- Hardware for sale
- Ransomware
- Loaders
- Counter antivirus service/checkers
- Hosting & infrastructure
- Recruiting for criminal groups

2 Distribution
- Social network and instant message spam
- Exploit kit development
- Spam email distribution
- Purchasing traffic and/or traffic distribution systems (TDS)

Vehicles delivering capabilities to victims

3 Monetization
Methods to capitalize on successfully executed capabilities

- Dump shops
- Collection and rackets
- Payment card information
- Money laundering
- Barter payments & extortion
Dump Shops & Sale of Payment Card Information
WHAT

- CrowdStrike has identified various formjacking campaigns likely from a single adversary
- Formjacking is a malicious JavaScript inject used to harvest payment or personal information from a web page
- The cluster uses consistent TTPs and distinctive JS to impersonate legitimate providers

SO WHAT?

- CrowdStrike assesses these campaigns are conducted by a single group
WHAT

- WIZARD SPIDER has been conducting formjacking campaigns to harvest payment card information.

SO WHAT?

- Formjacking is a new tactic for WIZARD SPIDER
- Previously they targeted POS devices with the Anchor framework to deploy MagneticScraper
- This pivot is likely spurred in part by decline of in-person retail due to COVID-19
Data Leak Sites
EMERGING TREND: DATA EXTORTION

**RECONNAISSANCE**
- Adversary conducts reconnaissance for domain controllers and valuable data

**EXFILTRATION**
- Sensitive corporate data is exfiltrated to adversary controlled off-site storage

**RANSOMWARE**
- Ransomware is deployed across enterprise-wide, including endpoints, network drives and shares

**EXTORTION**
- If ransom is not paid by deadline, actor extorts victim by threatening to release data

**CONSEQUENCES**
- If the victim refuses to pay extortion fee, actor follows through with their promise
INDUSTRIES AFFECTED BY DATA LEAKS

- Industries & Engineering
- Manufacturing
- Technology
- Retail
- Healthcare
- Financial Services
- Professional Services
- Government
- Logistics
- Legal
- Hospitality
- Energy
- Automotive
- Media
- Consumer Goods
- Nonprofit
- Academic
- Telecommunications
- Real Estate
- Agriculture
- Utilities
- Chemical
- Transportation
- Computer Gaming
- Aerospace
- Essential
- Automation
- Defense

Total

Graph showing the number of data leaks by industry.
Figure 4. Most Active BGH Adversaries with DLSs in 2020
WHAT?

• In March 2021, CrowdStrike Intelligence identified that GRACEFUL SPIDER has sent emails to third-party partners of their victims; the adversary likely obtained data from the original victims via the file transfer service Accellion FTA. These emails were used to notify the third parties their data was part of the Accellion FTA victim breach, with the likely intent to create negative publicity for their Accellion FTA victims.

SO WHAT?

• This recent campaign added an option for possibly affected third parties to purchase or remove the data from GRACEFUL SPIDER’s dedicated leak site (DLS). This option creates a way for GRACEFUL SPIDER to monetize campaigns in which their victims did not pay the ransom.
REVIL DATA LEAK SITE

WHAT
- PINCHY SPIDER is the group behind REvil
- They sell ransomware through a partnership program with a limited number of accounts.
- This model is known as “Ransomware-as-a-Service”

SO WHAT?
- CrowdStrike assesses they have 20-40 affiliates, but has recently launched a recruitment drive.
- Will ban users who do not deploy REvil on a regular basis
- Admin panel provides options to monitor and monetize REvil campaigns
WHAT

- Attempt to sell 13.6 GB of doc/video from the Uruguayan Navy
- This Activity observed on a Russian language forum
- Requested $500K of USD via crypto-currency
- Posted screen shots of “Navy confidential” documents

SO WHAT?

- Seller stated this data could be made available for sale on a data leak site (DLS)
- The referenced DLS belongs to PINCHY SPIDER operators of REvil ransomware
- At this time, the data has not been posted
PINCHY SPIDER

- Community Identifiers
  - GandCrab
  - REvil
  - Sodinokibi
  - GOLD GARDEN
  - GOLD SOUTHFIELD

REVIL DATA LEAK SITE
THE WAY FORWARD
YOUR ABILITY TO UNDERSTAND THE CRIMINAL ECOSYSTEM PUTS YOU IN A POSITION TO PROACTIVELY COMBAT THE ADVERSARY

**SERVICES**
Capabilities that enable eCrime activity

**DISTRIBUTION**
The vehicles through which capabilities are delivered to victims

**MONETIZATION**
The methods leveraged to capitalize on successful capability execution against victims
KEY RECOMMENDATIONS

INTELLIGENCE AUTOMATION
HIGH FIDELITY INDICATORS OF COMPROMISE
FALCON X STANDARD

INTELLIGENCE MONITORING
DARK WEB, BRAND PROTECTION, DATA LEAKS
FALCON X RECON

INTELLIGENCE REPORTING
GLOBAL THREAT INTELLIGENCE REPORTING
FALCON X PREMIUM

THREAT HUNTING
24/7, MANAGED, HUMAN-BASED THREAT HUNTING
OVERWATCH STANDARD

SERVICE PARTNER
SOLVE SKILLS SHORTAGE, RAPIDLY RESPOND TO THREATS
CROWDSTRIKE SERVICES
Your ability to defeat advanced cyber threats rests almost entirely on your understanding of the problem.
APPENDIX
FALCON X SOLUTION SUITE

FALCON X ELITE
- Assigned Elite Analyst
- Priority Intel Reqs
- Request for Intelligence
- Threat Graph Inquiries
- Personalized Briefings

FALCON X PREMIUM
- Intelligence Reports
- Malware Analysis
- YARA & Snort
- Tailored Intelligence

FALCON X STANDARD
- Endpoint Integration
- Malware Sandbox
- Indicators of Compromise
- Weekly Report
- Falcon Malquery
- Adversary Profiles

FALCON X RECON
- Open, Deep, & Dark Web
- Real-Time Monitoring
- Prioritized Alerts
- Universal Search
- Indicators of Compromise
- Adversary Profiles

Indicators of Compromise
Adversary Profiles
Real-Time Monitoring
Prioritized Alerts
Universal Search
Open, Deep, & Dark Web