ANOMALI

Cyber Threat Profile: Retail Sector

Source Statement: *This product is based on research utilizing various open and private sources, proprietary sources, and intelligence vendors. This Cyber Threat Profile report is based on collections and analysis that ended 23 OCT 2020.*

Overview

Anomali Threat Research conducted an analysis of numerous types of malicious cyber activity that affect the retail sector. Due to the complex nature of sophisticated threat actors and groups, in addition to economic and geopolitical factors that can motivate cyberattacks, this report will be broken down into sections to highlight specific threats and risks. The most prolific threat groups and most-observed tactics, techniques, and procedures (TTPs) used by threat actors will be discussed, as well as current geopolitical topics that contribute to and affect malicious cyber activity.

Cyber Landscape

The global retail sector has been significantly impacted by the COVID-19 pandemic, as some companies go out of business or temporarily suspend operations while others move to curbside pickup, online sales, or other creative business models. The retail market is predicted to fall from $21,821.4 billion (USD) to $21,622.6 billion in 2020 at a compound annual growth rate of –1%.[1] However, the global retail market is predicted to increase at a compound annual growth rate of 5% from 2021 to reach $25,122.2 billion in 2023.[2] The overall sales in the retail sector is estimated to be $4.89 trillion, decreasing from $5.47 trillion in 2019, and increase to $5.33 trillion in 2021.[3] The large monetary value, combined with known dates for online shopping such as Black Friday and Cyber Monday, represents the potential for significant illicit profit.

Many of the world's largest retail stores are pivoting resources to increase their stance in the burgeoning e-commerce sector. One such example is Walmart announcing the opening of its Walmart Marketplace in June 2020.[4] Other companies, such as Best Buy and Target, are also positioning themselves to move from brick-and-mortar locations to e-commerce sites.[5] With retail and e-commerce becoming more entwined, substantial sales volumes

provide a plethora of malicious opportunities. Global retail e-commerce sales in 2019 were $3.53 trillion, and are expected to increase to $6.54 trillion in 2022.[6] In addition to sales value, the retail sector also tends to employ younger individuals with less experience who need to be trained on cybersecurity protocols. However, even older and more experienced individuals are also in need of more cybersecurity training as threat actors continue to utilize new TTPs, and continue to use effective methods such as credential stuffing and spearphishing. Financially-motivated cybercrime actors cost the retail sector approximately $30 billion per year.[7]

While the COVID-19 pandemic has brought unprecedented changes to society, the effects on the cyber threat landscape have remained relatively minor.[8] Some of the changes in the cyber threat landscape post-COVID-19 include:[9]

- A shift from working in the office to remote locations exposes enterprise networks to a new type of threat.
- The use of COVID-19 topics and increase in health-themes for social engineering.
- Increase in the targeting of entities working in healthcare and healthcare-related manufacturing with cyberespionage objectives. In addition, these critical organizations are also increasingly vulnerable to ransomware attacks.

Threat Actors and Groups

There are multiple active and historic Advanced Persistent Threat (APT) groups and threat actors that target entities and individuals with various motivations and objectives. A larger list of threat groups that target the retail sector, including retail e-commerce, can be found in Appendix A. Awareness of these actors and their TTPs can assist in a proactive, rather than reactive, cyber strategy.

FIN7

The financially-motivated threat group FIN7 has been active since at least mid-2015 and has targeted various industries around the world with the objective of stealing financial data, primarily credit and debit card data. The group is Russian-speaking and operates on a global level. FIN7 is one of the most notorious financial groups, having been credited with the theft of over 15 million payment card records and causing organizations around the world approximately one billion dollars (USD) in losses.[10] In the United States (US) alone, the group has targeted over 100 companies and compromised the network of organizations in 47 states and the District of Columbia.[11] The group primarily targets high-usage Point-of-Sale (POS) terminals to steal payment card data and utilizes a mix of custom and open-source malware and tools to attack its targets. FIN7 also created a fake computer security company called Combi Security to serve as a front of legitimacy and to recruit members to participate in their malicious activities.[12] Combi Security is purportedly based in Russia and Israel.[13] The group engages in social engineering techniques ranging from custom phishing emails and documents to phone calls with store managers. The group will sell the financial data on various underground carding forums or utilize the information themselves for fraudulent activities.

On August 1, 2018, the US Department of Justice (DOJ) publicly announced the indictment of three members of FIN7. The indictment was issued for Ukrainian nationals Dmytro Fedorov, Fedir Hladyr, and Andrii Kolpakov for their part in FIN7 activity that targeted more than 100 U.S. companies and stole millions of credit and debit card data that was then used by the group or sold on underground forums for profit.[14] The arrest of the believed leaders of the financial threat group was thought to perhaps bring an end to FIN7 activity, or result in a new group filling a potential void. However, this notion is far

from accurate and FIN7 remains active at the time of this writing. FIN7 will also impersonate entities, most notably the US Securities and Exchange Commission (SEC), to make their spearphishing emails more likely to be read and malicious attachments opened.

The document file types range from DOC, RTF (sometimes with embedded LNKs) that typically contain a malicious macro that, if enabled, will launch obfuscated JavaScript. Sometimes the JavaScript is itself a backdoor, and other times the code will download other malware and tools such as the Carbanak data-stealing backdoor, a variant of the LaZagne credential recovery tool, the "Mimikatz" credential stealer, and custom malware such as DNSbot, PowerSource, and SQLRat.[15]

FIN8

FIN8 is a financially-motivated APT group that has been active since at least 2016.[16] The FIN8 group primarily targets the retail and hospitality industry and deploys POS malware to exfiltrate credit card details.[17] The group primarily relies on spearphishing emails to deliver weaponized macro-enabled documents to gain an initial foothold on their targets.[18] In the past, FIN8 has leveraged a zero-day vulnerability in its campaigns and also utilized innovative obfuscation techniques to effectively stay under the radar.[19]

The group spends a considerable amount of time performing reconnaissance on targets to send a tailored email.[20] The spearphishing email body will typically contain information about the target company such as their phone number, physical address, and name of the target. The specificity of information may increase the chances of a target opening the attachment.[21]

After the successful execution of the macro, the Visual Basic (VB) script utilizes Windows Management Instrumentation (WMIC) to execute a PowerShell script to download PunchBuggy malware. PunchBuggy is a Dynamic-Link Library (DLL) based downloader that can further download additional payloads from the Command and Control (C2) server.[22]

Mummy Spider

Aliases: *TA542*, *Emotet*, *Mealybug*, *Geodo*

The criminally-motivated threat group Mummy Spider was first identified by the security community in May 2014.[23] The group is associated with the well-known banking trojan Emotet (Geodo, Heodo) that originally targeted the customers of German and Austrian banks in 2014 and later spread across the UK, US, and other countries.[24] TA542 targets all industries on a global scale by distributing the Emotet trojan via wide-scale malspam campaigns with malicious attachments or links.[25] In 2017, Mummy Spider changed its operations from selling to acting as a malware distribution service for other malware, including IcedID, Gootkit, Trickbot among others.[26] The group is known for its modular architecture, persistence techniques, and worm-like capabilities to spread to other machines. These tactics show that the group is a highly innovative, sophisticated threat.[27]

Mummy Spider leverages large-scale malspam and phishing campaigns to distribute malware around the globe. The group utilizes social engineering tactics to increase infection rates. The emails are composed in language correlating to the targeted country and the email subjects usually refer to payments, transactions, and invoices.[28] Below are some social engineering techniques that are employed by Mummy Spider:[29]

- Brand Abuse
- Email Thread Hijacking
- Geographical Targeting
- Targeted Email subjects

Mummy Spider began their malicious operations solely utilizing the Emotet banking trojan to steal credentials of the targets. The group

later used Rig Exploit Kit (EK) to distribute the trojan in December 2016 and later changed to malspam emails.[30]

The Emotet malware has gone through several updates and improvements from its early operations that date back to 2014. It gains an initial foothold on a target machine by sending an email that contains either a malicious attachment or a URL that is used to download the malware into the target host. The malicious attachment types include, but are not limited to, the following:[31]

- JavaScript
- Microsoft Excel with macros
- Microsoft Word with macros
- Password protected Zip files
- PDF
- URLs

TA505

Aliases: *Graceful Spider, Gold Evergreen, TEMP. Warlock, Hive0065, Chimborazo*

The financially-motivated threat group called TA505 was first reported by Proofpoint researchers in December 2017.[32] Malicious activity attributed to the Russian-speaking group dates back to at least 2014, and the campaigns conducted by TA505 have targeted entities and individuals around the world. The group distributes a variety of malware, both well-known strains (Dridex banking trojan, Locky ransomware), custom-created (Jaff ransomware, tRAT), and variants of legitimate remote access tools (Remote Manipulator System). The group primarily distributes malware and tools via large-scale and indiscriminately-distributed malspam campaigns, often through the Necurs botnet, with malicious attachments or links. Incorporation of new malware, creating custom malware, and the use of advanced tactics, such as the removal of malware artifacts, indicate that this group is a sophisticated threat and likely well-funded. The group is innovative and shows the flexibility to pivot to other techniques and malware trends on a global scale.

TA505 conducts large-scale malspam campaigns that are distributed on a global level. The group has also been observed distributing malware in small, targeted campaigns with TA505 distributing custom malware like the group's FlawedAmmyy Remote Access Trojan (RAT), which was later used in more widespread campaigns.[33] The small-scale attacks typically target a financial institution with financially-themed malspam with the object of tricking email recipients into downloading malware (banking trojan, downloader, ransomware, RAT), typically by enabling malicious macros in an email attachment.[34] The group's malspam has also been observed to attempt to trick recipients into following a malicious link (sometimes shortened) or download a malicious archive.[35] The threat group will also use legitimately-signed certificates so the malware can impersonate legitimate software.

Wizard Spider

Aliases: *TheTrick, TrickBot*

Wizard Spider is a criminally-motivated threat group that operates the "Trickbot" botnet. The security community first identified the malware in September 2016, it is a successor of the Dyre malware family.[36] The threat group is believed to be operating out of Russia and actively maintains and develops the Trickbot botnet.[37] Trickbot is a well-known banking trojan that steals credentials, Personal Identifiable Information (PII), cryptocurrencies from the infected victims.[38] In August 2018, Ryuk ransomware targeted multiple large enterprises around the globe and demanded a hefty ransom from the victims. According to CrowdStrike, the Ryuk ransomware is operated by the threat actor Grim Spider, a subgroup of Wizard Spider.[39]

The Trickbot trojan spreads via large-scale malspam and phishing campaigns to distribute

malware around the globe. The group utilizes social engineering tactics to increase infection rates. The emails are composed in language correlating to the targeted country and the email subjects usually referred to payments, bank transaction receipts, and invoices. Listed below are some social engineering techniques that are employed by Wizard Spider:[40]

- Brand Abuse
- Geographical Targeting
- Tax Notices
- Targeted Email subjects

Trickbot has gone through several updates and improvements from its early operations dating back to 2016. The malware began its operations as a banking trojan and later incorporated multiple modules to perform other malicious activities like credential stealing and worm-like capability.[41] The variants of Trickbot have modules as mentioned below in their architecture:[42]

- importDll64
- injectDll64
- networkDll64
- newBCtestDll64
- psfin64
- pwgrab64
- sharedll64
- systeminfo64
- vncDll64
- wormDll64

Industry Targeting

The retail sector, and their associated e-commerce sites, is one of the most heavily targeted industries and suffered the most data breaches of any industry in 2019.[43] The large amount of incidents affecting retail organizations comes after large-scale data breaches affected numerous individuals when their personally identifiable information (PII) and financial data were leaked by large companies such as JPMorgan, Home Depot, and Target in 2014.[44] These incidents prompted then US President Barack Obama to sign an executive order, called Improving the Security of Consumer Financial Transactions, to implement chip and pin technology to protect customer information.[45] This order is important because as chip and pin technology became widely-implemented some threat actors searched for a new way to steal sensitive information, such as the websites that process payment card data instead of POS terminals. An example of these changing TTPs can be observed in Trustwave researchers' findings that threat actors attempted to steal card-not-present (CNP) data, which usually occurs during online transactions, 77% of the time data was targeted in an attack on retail.[46]

Threat actors that target retail are often financially motivated, and such actors can be tenacious in their attempts to make an illicit profit. In addition, as consumer ease-of-use and technology move shopping to online stores, threat actors pivot their targeting as well. Furthermore, researchers predict retailers to lose approximately $130 billion to CNP data theft between 2018 and 2023.[47] Nevertheless, governments have taken steps to improve the protection of customer information and hold organizations responsible for handling sensitive information. The standard for security protocols is the General Data Protection Regulation (GDPR) that was implemented by the European Union (EU) on May 25, 2018.[48]

Common Attack Vectors and TTPs

Threat actors target numerous infection vectors utilizing various TTPs that can differ depending on the threat group, their motivations, and their sophistication. However, amongst the plethora of actors, malware, tools, and TTPs, there are commonalities and similarities that can be

observed in malicious cyber actors targeting the retail sector.

Attack Vectors

The most common attack vectors threat actors utilize or target consist of, but are not limited to, the following:[49]

- Card readers / POS terminals
- Credential stuffing
- Near field communication (NFC)
- Phishing
- RAM scraping
- Social engineering
- Spearphishing
- Web skimming
  - Command injection
  - Cookie poisoning
  - Directory traversal (file-path traversal)
  - SQL injection

Malware

The most common malware threat actors use to target the retail sector include, but is not limited to, is shown in Table 1 below.

Table 1. Common Malware and Tools Targeting the Retail Sector[50]

Malware	Description
Emotet	A modular banking trojan that typically functions as a dropper for other malware.[51]
Gh0stRAT	Remote access tool that is used by, and has had variants created, multiple threat actors.[52]
Kryptik	Malware family of trojans that are capable of collecting system information, downloading and uploading files, and use anti-analysis techniques.[53]
Magecart	Referring to data-stealing scripts injected into websites used by threat actors to steal payment data, often targeting Magento-based websites.[54]
njRAT (LV, Bladabindi)	Remote access tool used by multiple groups that are primarily located in the Middle East.[55]
Obfuse	Information-stealing trojan.[56]
Sogou	Adware named after the Chinese search engine, Sogou.[57]
Trickbot	Banking trojan that is used to steal financial data from websites.[58]
WannaCry (WannaCrypt)	Ransomware responsible for the global campaign in 2017 that targets out-of-date Windows systems and has propagates through the SMBv1 exploit, EternalBlue.[59]
XtremeRAT	Multi-functional remote access trojan whose leaked source code has been used for many other malware variants.[60]

Common TTPs

The most common TTPs threat actors use to target the retail sector include, but are not limited to, the following:

- Application Layer Protocol: Web Protocols
- Bypass User Access Control
- Code Signing
- Command and Scripting Interpreter: Visual Basic
- Create or Modify System Process: Windows Service
- Credential stuffing
- Cross-site scripting
- Defense Evasion
- Encrypted Channel: Asymmetric Cryptography
- Exploitation for Client Execution
- Exploitation for Privilege Escalation
- Indicator Removal on Host: File Deletion
- Ingress Tool Transfer
- Inter-Process Communication: Dynamic Data Exchange
- Logon Script (Windows)
- Malicious File
- Network Service Scanning
- Obfuscated Files or Information
- Phishing
- Process Injection
- Protocol Tunneling
- Registry Run Keys / Startup Folder
- Remote Access Software
- Remote Services: Remote Desktop Protocol
- Scheduled Task/Job
- Scripting
- Security Software Discovery
- Social engineering
- Software Discovery
- Spearphishing attachment
- Spearphishing Link
- template injection
- User Execution
- Valid Accounts
- XSL Script Processing

Conclusion

The retail cyber threat landscape faces numerous risks, from physical POS terminals and work machines to retailers' increasing dependence on e-commerce that opens more attack vectors for threat actors. However, there has been great progress in protecting individuals' sensitive information that has been passed in multinational agreements, such as GDPR. Organizations are beginning to see the value in taking necessary steps to begin developing cyber and information security strategies and policies. In addition, awareness of threat actors and the malware and TTPs they utilize can assist in creating a more proactive rather than reactive cybersecurity posture.

Endnotes

1 "Global Retail Market Report (2020 to 2030) – COVID-19 Impact and Recovery," GlobeNewswire, accessed October 12, 2020, published May 14, 2020, https://www.globenewswire.com/news-release/2020/05/14/2033483/0/en/Global-Retail-Market-Report-2020-to-2030-COVID-19-Impact-and-Recovery.html#:~:text=The%20global%20retail%20market%20is,CAGR)%20of%20%2D1%25.

2 Ibid.

3 Statista Research Department, "Total U.S. retail Sales 2012-2024," Statista, accessed October 12, 2020, published August 28, 2020, https://www.statista.com/statistics/443495/total-us-retail-sales/#:~:text=Total%20retail%20sales%20in%20the,result%20of%20the%20coronavirus%20pandemic.

4 "Walmart Expands Its eCommerce Marketplace to More Small Businesses," Walmart, accessed October 12, 2020, published June 15, 2020, https://corporate.walmart.com/newsroom/2020/06/15/walmart-expands-its-ecommerce-marketplace-to-more-small-businesses.

5 Mallika Mitra, "Price wars and e-commerce investment to weigh on retailer profits, Moody's says," CNBC, accessed October 12, 2020, published November 1, 2019, https://www.cnbc.com/2019/11/01/retail-profits-to-take-a-hit-from-price-wars-and-investments-moodys-says.html.

6 J. Clement, "Global retail e-commerce sales 2014-2023," Statista, https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/.

7 "Cyber(attack) Monday: Hackers Target the Retail Industry as E-Commerce Thrives," IntSights, accessed October 12, 2020, published December 2019, https://wow.intsights.com/rs/071-ZWD-900/images/Cyber%20Attack%20Monday.pdf, 2.

8 Gage Mele, Parthiban R., and Tara Gould, "COVID-19 Themes Are Being Utilized by Threat Actors of Varying Sophistication," Anomali Blog, accessed October 12, 2020, published March 23, 2020, https://www.anomali.com/blog/covid-19-themes-are-being-utilized-by-threat-actors-of-varying-sophistication; Tara Gould, Gage Mele, Parthiban Rajendran, and Rory Gould, "Anomali Threat Research Identifies Fake COVID-19 Contact Tracing Apps Used to Download Malware that Monitors Devices, Steals Personal Data," Anomali Blog, accessed October 12, 2020, published June 10, 2020, https://www.anomali.com/blog/anomali-threat-research-identifies-fake-covid-19-contact-tracing-apps-used-to-monitor-devices-steal-personal-data; Sandra Joyce, "Limited Shifts in the Cyber Threat Landscape Driven by COVID-19," FireEye Blog, accessed October 12, 2020, published April 8, 2020, https://www.fireeye.com/blog/threat-research/2020/04/limited-shifts-in-cyber-threat-landscape-driven-by-covid-19.html

9 Ibid.

10 Jeremy Kirk, "Feds Announce Arrests of 3 'FIN7' Cybercrime Gang Members," BankInfoSecurity, accessed October 12, 2020, published August 2, 2018, https://www.bankinfosecurity.com/three-arrested-in-large-payment-card-hacking-scheme-a-11272.

11 Office of Public Affairs, "Three Members of Notorious International Cybercrime Group "Fin7" In Custody for Role in Attacking Over 100 U.S. companies," The US Department of Justice, accessed October 13, 2020, published August 1, 2018, https://www.justice.gov/opa/pr/three-members-notorious-international-cybercrime-group-fin7-custody-role-attacking-over-100.

12 Office of Public Affairs, "HOW FIN7 ATTACKED AND STOLE DATA," the US Department of Justice, accessed October 13, 2020, https://www.justice.gov/opa/press-release/file/1084361/download.

13 Joshua Platt and Jason Reaves, "FIN7 Revisited: Inside Astra Panel and SQLRat Malware," Flashpoint Blog, accessed October 13, 2020, published March 20, 2019, https://www.flashpoint-intel.com/blog/fin7-revisited-inside-astra-panel-and-sqlrat-malware/.

14 Office of Public Affairs, "HOW FIN7 ATTACKED AND STOLE DATA," the US Department of Justice.

15 Steve Miller et al., "FIN7 Spear Phishing Campaign Targets Personnel Involved in SEC Filings"; Mathew McWhirt et al., "To SDB, Or Not To SDB: FIN7 Leveraging Shim Databases for Persistence," FireEye Blog, accessed October 13, 2020, published Mar 3, 2017, https://www.fireeye.com/blog/threat-research/2017/05/fin7-shim-databases-persistence.html; Joshua Platt and Jason Reaves, "FIN7 Revisited Inside Astra Panel and SQLRat Malware"; Michael Gorelik, "MORPHISEC DISCOVERS NEW FILELESS ATTACK FRAMEWORK," Morphisec Blog, accessed October 13, 2020, published March 16, 2017, http://blog.morphisec.com/fileless-attack-framework-discovery.

16 Kristina Savelesky, et al., "ABADBABE 8BADF00D: Discovering BADHATCH and a Detailed Look at FIN8's Tooling," Gigamon Blog, accessed October 13, 2020, published July 23, 2019, https://atr-blog.gigamon.com/2019/07/23/abadbabe-8badf00d-discovering-badhatch-and-a-detailed-look-at-fin8s-tooling/.

17 Michael Gorelik, "FIN8 IS BACK IN BUSINESS TARGETING THE HOSPITALITY INDUSTRY," Morphisec Blog, accessed October 13, 2020, published June 10, 2019, https://blog.morphisec.com/security-alert-fin8-is-back.

18 Josh Grunzweig and Brandon Levene, "PowerSniff Malware Used in Macro-based Attacks," Palo Alto Networks, accessed October 14, 2020, published March 11, 2016, https://unit42.paloaltonetworks.com/powersniff-malware-used-in-macro-based-attacks.

19 Dhanesh Kizhakkinan, et al., "Threat Actor Leverages Windwos Zero-day Exploit in Payment Card Data Attacks," FireEye Blog, accessed October 14, 2020, published May 11, 2016, https://www.fireeye.com/blog/threat-research/2016/05/windows-zero-day-payment-cards.html.

20 Ibid.

21 Josh Grunzweig and Brandon Levene, "PowerSniff Malware Used in Macro-based Attacks," Palo Alto Networks.

22 Ibid.
23 Axel F and the Proofpoint Threat Insight Team, "Threat Actor Profile: TA542, From Banker Malware to Malware Distribution Service," Proofpoint, accessed October 14, 2020, published May 15, 2019, https://www.proofpoint.com/uk/threat-insight/post/threat-actor-profile-ta542-banker-malware-distribution-service.
24 "Emotet Changes TTPs and Arrives in the United States," Center for Internet Security Blog, accessed October 14, 2020, published April 27, 2017, https://www.cisecurity.org/blog/emotet-changes-ttp-and-arrives-in-united-states/.
25 ESET Research, "Emotet launches major new spam campaign," WeLiveSecurity, accessed October 14, 2020, published November 9, 2018, https://www.welivesecurity.com/2018/11/09/emotet-launches-major-new-spam-campaign.
26 "The Evolution of Emotet: From Banking Trojan to Threat Distributor," Symantec Enterprise Blog, accessed October 14, 2020, published July 18, 2018, https://www.symantec.com/blogs/threat-intelligence/evolution-emotet-trojan-distributor.
27 "Let's talk Emotet Malware," Malwarebytes, accessed October 14, 2020, https://www.malwarebytes.com/emotet.
28 Axel F and the Proofpoint Threat Insight Team, "Threat Actor Profile: TA542, From Banker Malware to Malware Distribution Service," Proofpoint.
29 Ibid.
30 Ibid.
31 Ibid.
32 "Threat Actor Profile: TA505, From Dridex to GlobeImposter," Proofpoint, accessed October 14, 2020, published September 27, 2020, https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta505-dridex-globeimposter.
33 Tom Spring, "TA505 Crooks are Now Targeting US Retailers with Personalized Campaigns," Threatpost, accessed October 15, 2020, published December 7, 2018, https://threatpost.com/ta505-crooks-are-now-targeting-us-retailers-with-personalized-campaigns/139702/.
34 Lindsey O'Donnell, "Unique Malspam Campaign Uses MS Publisher to Drop a RAT on Banks," Threatpost, accessed October 15, 2020, published August 17, 2018, https://threatpost.com/unique-malspam-campaign-uses-ms-publisher-to-drop-a-rat-on-banks/136656/.
35 "A deep insight into the prolific TA505 Threat Actor Group's massive campaigns," Cyware, accessed October 15, 2020, published February 2, 2019, https://cyware.com/news/a-deep-insight-into-the-prolific-ta505-threat-actor-groups-massive-campaigns-53967575.
36 "TrickBot: We Missed you, Dyre," Fidelis, accessed October 15, 2020, published October 15, 2016, https://www.fidelissecurity.com/threatgeek/archive/trickbot-we-missed-you-dyre/.
37 "WIZARD SPIDER," Malpedia, accessed October 15, 2020, https://malpedia.caad.fkie.fraunhofer.de/actor/wizard_spider.
38 Roland Dela Paz, "Trickbot goes after cryptocurrency," Forcepoint blog, accessed October 15, 2020, published August 29, 2017, https://www.forcepoint.com/blog/x-labs/trickbot-goes-after-cryptocurrency.
39 Alexander Hanel, "Big Game Hunting with Ryuk: Another Lucrative Targeted Ransomware," Crowdstrike Blog, accessed October 15, 2020, published January 10, 2019, https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/.
40 Axel F and the Proofpoint Threat Insight Team, "Threat Actor Profile: TA542, From Banker Malware to Malware Distribution Service," Proofpoint.
41 Mark, "TRICKBOT – Analysis," Sneakymonkey, accessed October 15, 2020, published May 22, 2019, https://www.sneakymonkey.net/2019/05/22/trickbot-analysis/.
42 Ibid.
43 "New Trustwave Report Reveals Cybersecurity Threats Becoming Pervasive and Attacks More Targeted," Trustwave, accessed October 15, 2020, published April 22, 2020, https://www.trustwave.com/en-us/company/newsroom/news/new-trustwave-report-reveals-cybersecurity-threats-becoming-pervasive-and-attacks-more-targeted/; "Cyber(attack) Monday: Hackers Target the Retail Industry as E-Commerce Thrives," IntSights, 2.
44 Sarah N. Lynch and Steve Holland, "Obama signs order to tighten security for federal credit cards," Reuters, accessed October 15, 2020, published October 17, 2014, https://www.reuters.com/article/us-obama-credit-security/obama-signs-order-to-tighten-security-for-federal-credit-cards-idUSKCN0I61OP20141017.
45 Ibid.; Office of the Press Secretary, "Executive Order –Improving the Security of Consumer Financial Transactions," The White House, accessed October 15, 2020, published October 17, 2014, https://obamawhitehouse.archives.gov/the-press-office/2014/10/17/executive-order-improving-security-consumer-financial-transactions.
46 "Cyber(attack) Monday: Hackers Target the Retail Industry as E-Commerce Thrives," IntSights, 3.
47 "RETAILERS TO LOSE $130BN GLOBALLY IN CARD-NOT-PRESENT FRAUD OVER THE NEXT 5 YEARS," Juniper Research, accessed October 16, 2020, published January 2, 2019, https://www.juniperresearch.com/press/press-releases/retailers-to-lose-130-bn-globally-in-card-fraud.
48 "General Data Protection Regulation GDPR," Intersoft Consulting, accessed October 16, 2020, https://gdpr-info.eu/.
49 Kayla Matthews, "6 ways hackers targeting retail businesses," Malwarebytes Blog, accessed October 16, 2020, published January 8, 2020, https://blog.malwarebytes.com/web-threats/2020/01/6-ways-hackers-are-targeting-retail-businesses/; Segun Onibalusi, "4 security threats retailers should watch out for during the rest of 2020," Digital Commerce 360, accessed October 16, 2020, published May 1, 2020, https://www.digitalcommerce360.com/2020/05/01/4-security-threats-retailers-should-watch-out-for-during-the-rest-of-2020/.

50 "2020 State of Malware Report," Malwarebytes Labs, accessed October 16, 2020, published February 2020, https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report-1.pdf, 49-50; "CYBER THREATS TO THE RETAIL AND CONSUMER GOOD INDUSTRY," FireEye, accessed October 16, 2020, https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/ib-retail-consumer.pdf.

51 "Emotet," MITRE | ATT&CK, https://attack.mitre.org/software/S0367/; "Emotet Malware," US-CERT, accessed October 19, 2020, published January 23, 2020, https://us-cert.cisa.gov/ncas/alerts/TA18-201A.

52 "gh0st RAT," MITRE | ATT&CK, https://attack.mitre.org/software/S0032/.

53 "Threat Roundup for May 3 to May 10," Cisco Talos Blog, accessed October 19, 2020, published May 10, 2019, https://blog.talosintelligence.com/2019/05/threat-roundup-0503-0510.html; "TROJAN.WIN32.KRYPTIK," Kaspersky Threats, accessed October 19, 2020, https://threats.kaspersky.com/en/threat/Trojan.Win32.Kryptik/.

54 "Inside Magecart," RiskIQ and Flashpoint, accessed October 20, 2020, published November 2018, https://cdn.riskiq.com/wp-content/uploads/2018/11/RiskIQ-Flashpoint-Inside-MageCart-Report.pdf, 2, 5, 8.

55 "njRAT," MITRE | ATT&CK, https://attack.mitre.org/software/S0385/.

56 "2020 CYBER THREAT INTELLIGENCE ESTIMATE," Optiv, accessed October 20, 2020, published August 2020, https://www.optiv.com/sites/default/files/2020-08/TL_2020-CTIE-Report_Whitepaper.pdf, 18.

57 "Adware.Sogou," Malwarebytes Blog, https://blog.malwarebytes.com/detections/adware-sogou/.

58 "TrickBot," MITRE | ATT&CK, https://attack.mitre.org/software/S0266/.

59 "WannaCry," MITRE | ATT&CK, https://attack.mitre.org/software/S0366/.

60 "Threat Roundup for February 21 to February 28," Cisco Talos Blog, accessed October 21, 2020, published February 28, 2020, https://blog.talosintelligence.com/2020/02/threat-roundup-0221-0228.html.

61 "APT32," ThreatStream, https://ui.threatstream.com/actor/1465.

62 "APT41," ThreatStream, https://ui.threatstream.com/actor/28033.

63 "Bamboo Spider," ThreatStream, https://ui.threatstream.com/actor/27832.

64 "How the Nasty Netwalker Behaved in Past Few Months," CyWare, https://cyware.com/news/how-the-nasty-netwalker-behaved-in-past-few-months-257c8217.

65 Michael Gorelik, "MOVING TARGET DEFENSE BLOG," Morphisec Blog, accessed October 21, 2020, published October 8, 2018, https://blog.morphisec.com/cobalt-gang-2.0; "Threat Group Cards: A Threat Actor Encyclopedia," ThaiCERT, accessed October 21, 2020, published July 8, 2020, https://www.dropbox.com/s/ds0ra0c8odwsv3m/Threat%20Group%20Cards.pdf?dl=0, 85.

66 Brett Stone-Gross, et al., "BitPaymer Source Code Fork: Meet DoppelPaymer Ransomware and Dridex 2.0," Crowdstrike Blog, accessed October 21, 2020, published July 12, 2019, https://www.crowdstrike.com/blog/doppelpaymer-ransomware-and-dridex-2/; "Threat Group Cards: A Threat Actor Encyclopedia," ThaiCERT, 393.

67 "Evil Corpt," ThreatStream, https://ui.threatstream.com/actor/27798.

68 "FIN5," ThreatStream, https://ui.threatstream.com/actor/14711.

69 Morphisec Labs, "NEW GLOBAL CYBER ATTACK ON POINT OF SALE SYSTEMS," Morphisec Blog, accessed October 21, 2020, published February 27, 2019, https://blog.morphisec.com/new-global-attack-on-point-of-sale-systems; Brendan McKeague, "Pick-Six: Intercepting a FIN6 Intrusion, an Actor Recently Tied to Ryuk and LockerGoga Ransomware," FireEye Blog, accessed October 21, 2020, published April 5, 2019, https://www.fireeye.com/blog/threat-research/2019/04/pick-six-intercepting-a-fin6-intrusion.html.

70 "FIN7," ThreatStream, https://ui.threatstream.com/actor/1731.

71 "FIN8," ThreatStream, https://ui.threatstream.com/actor/14714.

72 Alexander Hanel, "Big Game Hunting with Ryuk: Another Lucrative Targeted Ransomware," Crowdstrike Blog.

73 A L Johnson, "Hidden Lynx – Professional Hackers for Hire," Broadcom Blog, accessed October 22, 2020, published September 17, 2013, https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=8962de07-8e6a-41cc-a6d6-d22ea52dcbfa&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments.

74 "MageCart," ThreatStream, https://ui.threatstream.com/actor/21764.

75 "Mummy Spider," ThreatStream, https://ui.threatstream.com/actor/27288.

76 "Pinchy Spider," ThreatStream, https://ui.threatstream.com/actor/27936.

77 Alex Orleans, "Who Is PIONERR KITTEN?" Crowdstrike Blog, accessed October 23, 2020, published August 31, 2020, https://www.crowdstrike.com/blog/who-is-pioneer-kitten/.

78 "TA505," ThreatStream, https://ui.threatstream.com/actor/26092.

79 "TA544," ThreatStream, https://ui.threatstream.com/actor/27912.

80 "DanaBot – A new banking Trojan surfaces Down Under," Proofpoint, accessed October 23, 2020, published May 31, 2018, https://www.proofpoint.com/us/threat-insight/post/danabot-new-banking-trojan-surfaces-down-under-0.

81 "2019 GLOBAL THREAT REPORT," Crowdstrike, accessed October 22, 2020, https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2019GlobalThreatReport.pdf, 55.

82 "Turla," ThreatStream, https://ui.threatstream.com/actor/1145.

83 "Wizard Spider," ThreatStream, https://ui.threatstream.com/actor/27829.

Appendix A

Table 2. Threat Groups that Target the Retail Industry

Threat Actor/Group	Description	Country of Origin
APT32 (OceanLotus, SeaLotus, APT-C-00, Ocean Buffalo)	Cyberespionage group that targets numerous industries with commodity and custom malware since at least 2013.[61]	Vietnam
APT41	Sophisticated group that engages in cyberespionage and financially-motivated campaigns.[62]	China
Bamboo Spider (Panda Zeus, Panda Banker, Zeus Panda)	Financially-motivated group known for creating the Panda Banker (PandaBot, Zeus Panda) commodity banking trojan.[63]	Unknown
Circus Spider	Cybercriminal group that develops and operates the NetWalker ransomware.[64]	Unknown
Cobalt Group (Cobalt Spider, Cobalt Gang, Gold Kingswood)	Financially-motivated threat groups that have attacked entities in multiple sectors with a variety of malware and tools.[65]	Russia
Doppel Spider	Cybercriminal group that appears to some association with Indrik Spider, which is a subgroup of TA505.[66]	Russia
Evil Corp (Indrik Spider)	Sophisticated cybercriminal group that operates the Dridex botnet.[67]	Russia
FIN5	Financially-motivated group that primarily uses compromised credentials as their initial infection vector.[68]	Unknown
FIN6 (Skeleton Spider)	Financially-motivated group known for targeting point-of-sale (PoS) systems around the world.[69]	Unknown
FIN7	Sophisticated group that targets numerous sectors primarily located in Europe and the US.[70]	Russia
FIN8	Financially-motivated group that primarily targets the retail and hospitality industries in North America.[71]	Unknown
Grim Spider	Subgroup of Wizard Spider that operates targeted Ryuk ransomware campaigns.[72]	Russia
Hidden Lynx	Cyberespionage group that offers "professional hackers for hire."[73]	China
Magecart	The umbrella term, Magecart, refers to groups that target online commercial websites and inject payment skimming scripts to illicitly obtain credit card credentials.[74]	Unknown

Threat Actor/Group	Description	Country of Origin
Mummy Spider (TA542, Emotet, Mealybug, Geodo)	Financially-motivated group that operates the Emotet botnet.[75]	Unknown
Pinchy Spider (Gold Southfield, Gold Garden)	Ransomware-as-a-service group that operates GandCrab, and later Sodinokibi (REvil).[76]	Russia
Pioneer Kitten (Parasite, UNC757, Fox Kitten)	Information-motivated group that targets a variety of industries with the objective of maintaining a presence on target networks.[77]	Iran
TA505 (Graceful Spider, Gold Evergreen, TEMP. Warlock, Hive0065, Chimborazo)	Financially-motivated threat group that distributes commodity and custom malware.[78]	Unknown
TA544 (Cutwail V2, Narwhal Spider)	Financially-motivated group and the criminal operator of the Cutwail botnet version 2 (Cutwail V2).[79]	Unknown
TA547 (Scully Spider)	Financially-motivated threat group known for using commodity malware, such as DanaBot.[80]	Unknown
Tiny Spider	Financially-motivated motivated group behind the TinyLoader and TinyPOS malware.[81]	Unknown
Turla (Waterbug, Venomous Bear, Group 88, SIG23, Iron Hunter, Pacifier APT)	Connected to the "Epic" cyber-espionage campaign that targets government agencies around the globe, and is also connected to the Agent.btz worm that infected the network of the U.S. Department of Justice in 2008.[82]	Russia
Wizard Spider (TheTrick, TrickBot)	Financially-motivated group that operates targeting campaigns using Ryuk ransomware and develops the Trickbot botnet.[83]	Russia