NOTABLE RECENT SECURITY ISSUES

SELECTED BY THE TALOS SECURITY INTELLIGENCE AND RESEARCH GROUP

Title: **New Xbash malware targets Windows, Linux systems**
Description: Researchers discovered a new malware family known as “Xbash” in the wild targeting Windows and Linux systems. Xbash combines features of ransomware and cryptocurrency miners and has the ability to self-propagate. The malware spreads by attacking weak passwords and existing software vulnerabilities.
Reference: **https://researchcenter.paloaltonetworks.com/2018/09/unit42-xbash-combines-botnet-ransomware-coinmining-worm-targets-linux-windows/**
Snort SID: 47866 - 47873

Title: **Adobe discloses bugs in Acrobat and Reader**
Description: Adobe released security updates for Acrobat and Reader for Windows and MacOS. Successful exploitation of the critical and important vulnerabilities could lead to arbitrary code execution.
Reference: **https://helpx.adobe.com/security/products/acrobat/apsb18-34.html**
Snort SID: 47852 - 47857, 47883, 47884

Title: **Three important vulnerabilities in Cisco Webex**
Description: Multiple bugs exist in Cisco Webex Network Recording Player for Advanced Recording Format that could allow an attacker to execute arbitrary code on a targeted system. The vulnerabilities lie in the way that Webex handles recorded files.
Reference: **https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180919-webex**
Snort SID: 47878 - 47879

INTERESTING NEWS FROM AROUND THE SECURITY COMMUNITY

The creators of the Mirai botnet avoided jail time by striking a deal with prosecutors and agreeing to work with the FBI to fight cybercrime.
https://www.wired.com/story/mirai-botnet-creators-fbi-sentencing/

Government Payment Service Inc. — a popular website for individuals to pay for government services and fines — leaked more than 14 million customers’ records.
https://krebsonsecurity.com/2018/09/govpaynow-com-leaks-14m-records/

The U.K. is preparing to establish a new agency that will regulate the use of the internet, including implementing age restrictions for social media.
https://www.buzzfeed.com/alexwickham/uk-government-regulator-internet

The White House released a new plan that outlines ways in which the U.S. hopes to go on the offensive with is cyber capabilities — including targeting Russia.
https://www.cyberscoop.com/white-house-cyber-strategy-john-bolton-announcement/

Online retailer Newegg suffered a month long data breach that impacted customers’ credit card information, the same attack that recently targeted British Airways and Ticketmaster U.K.
https://www.theverge.com/2018/9/19/17879630/newegg-user-credit-card-info-data-breach-hack

The U.S. State Department’s classified email server was recently hacked. A spokesperson for the agency says that less than 1 percent of employees’ inboxes were breached.
https://www.cnn.com/2018/09/17/politics/state-department-email-breach/index.html

Japanese cryptocurrency exchange Zaif lost $60 million worth of digital coins in an attack.
http://fortune.com/2018/09/20/cryptocurrency-exchange-hack-zaif-japan-60-million/

RECENT VULNERABILITIES FOR WHICH EXPLOITS ARE AVAILABLE

COMPILED BY THE QUALYS VULNERABILITY RESEARCH TEAM

This is a list of recent vulnerabilities for which exploits are available. System administrators can use this list to help in prioritization of their remediation activities. The Qualys Vulnerability Research Team compiles this information based on various exploit frameworks, exploit databases, exploit kits and monitoring of internet activity.

ID: CVE-2018-11776
Title: **Apache Struts 2 Namespace Remote Code Execution Vulnerability (S2-057)**
Vendor: Apache Software Foundation
Description: Apache Struts versions 2.3 to 2.3.34 and 2.5 to 2.5.16 suffer from possible Remote Code Execution when using results with no namespace and in same time, its upper action(s) have no or wildcard namespace. Same possibility when using url tag which doesn't have value and action set and in same time, its upper action(s) have no or wildcard namespace.
CVSS v2 Base Score: 10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

ID: CVE-2018-2628
Title: **Oracle Weblogic Deserialization Remote Code Execution Vulnerability**
Vendor: Oracle
Description: Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0, 12.1.3.0, 12.2.1.2 and 12.2.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server.
CVSS v2 Base Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

ID: CVE-2018-8174
Title: **Windows VBScript Engine Remote Code Execution Vulnerability**
Vendor: Microsoft
Description: The VBScript engine contains a remote code execution vulnerability due to how it handles objects in memory. An attacker could execute arbitrary code in the context of the current user.
CVSS v2 Base Score: 7.6 (AV:N/AC:H/Au:N/C:C/I:C/A:C)

ID: CVE-2018-7600
Title: **Drupal Core Remote Code Execution Vulnerability (SA-CORE-2018-002)**
Vendor: Drupal
Description: Drupal before 7.58, 8.x before 8.3.9, 8.4.x before 8.4.6, and 8.5.x before 8.5.1 allows remote attackers to execute arbitrary code because of an issue affecting multiple subsystems with default or common module configurations.
CVSS v2 Base Score: 10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

ID: CVE-2018-0886
Title: **Microsoft Credential Security Support Provider Remote Code Execution Vulnerability**
Vendor: Microsoft
Description: The Credential Security Support Provider protocol (CredSSP) in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709 Windows Server 2016 and Windows Server, version 1709 allows a remote code execution vulnerability due to how CredSSP validates request during the authentication process, aka "CredSSP Remote Code Execution Vulnerability".
CVSS v2 Base Score: 7.6 (AV:N/AC:H/Au:N/C:C/I:C/A:C)

ID: CVE-2018-4878
Title: **Adobe Flash Player Remote Code Execution Vulnerability (APSA18-01)**
Vendor: Adobe
Description: A critical vulnerability exists in Adobe Flash Player 28.0.0.137 and earlier versions. Successful exploitation could potentially allow an attacker to take control of the affected system. Adobe is aware of a report that an exploit for CVE-2018-4878 exists in the wild and is being used in targeted attacks.
CVSS v2 Base Score: 10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

ID: CVE-2017-12636
Title: **Apache CouchDB Remote Code Execution Vulnerability**
Vendor: Apache Software Foundation
Description: CouchDB administrative users can configure the database server via HTTP(S). Some of the configuration options include paths for operating system-level binaries that are subsequently launched by CouchDB. This allows an admin user in Apache CouchDB before 1.7.0 and 2.x before 2.1.1 to execute arbitrary shell commands as the CouchDB user, including downloading and executing scripts from the public internet.
CVSS v2 Base Score: 9.0 (AV:N/AC:L/Au:S/C:C/I:C/A:C)

ID: CVE-2017-10271
Title: **Oracle WebLogic WLS Security Component Remote Code Execution**
Vendor: Oracle
Description: Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Security). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.1.0 and 12.2.1.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle

WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server.
CVSS v2 Base Score: 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

MOST PREVALENT MALWARE FILES September 20 - 27, 2018
COMPILED BY TALOS SECURITY INTELLIGENCE AND RESEARCH GROUP

SHA 256: d8647dfb73ad636c7c1a743754b47ff1824c11cfef040104efabca92715ffcff1
MD5: f174283dc138a4e412afbb3395d4288f
VirusTotal:
https://www.virustotal.com/#/file/d8647dfb73ad636c7c1a743754b47ff1824c11cfef040104efabca92715ffcff/details
Typical Filename: maftask.zip
Claimed Product: N/A
Detection Name: OSX.D8647DFB73.agent.tht.Talos

SHA 256: 2730b9afbda5db068b8736e49b329e49aa0156b30180af2fa7bb178151e17a0a
MD5: 14c543a105c1b089879d5eb7a8ac45f1
VirusTotal:
https://www.virustotal.com/#/file/2730b9afbda5db068b8736e49b329e49aa0156b30180af2fa7bb178151e17a0a/details
Typical Filename: ServicePlug.zip
Claimed Product: N/A
Detection Name: W32.2730B9AFBD-87.SBX.VIOC

SHA 256: 253676d93e6b79d119c99967e407926052df8b5520948069a2cac5e9ec5c7a7f
MD5: cbdef3b550a24cdfbb96a7501337a14f
VirusTotal:
https://www.virustotal.com/#/file/253676d93e6b79d119c99967e407926052df8b5520948069a2cac5e9ec5c7a7f/details
Typical Filename: diantz.exe
Claimed Product: Microsoft Cabinet Maker
Detection Name: Win.Trojan.Emotet.hunt.Talos

SHA 256: c59ac374df03908a863bb5e2a8cfd911b788f9751b4d5d4d075f013b75195217
MD5: be4e947c89ee40058f37534c4a3d3f34
VirusTotal:
https://www.virustotal.com/#/file/c59ac374df03908a863bb5e2a8cfd911b788f9751b4d5d4d075f013b75195217/details
Typical Filename: helperamc.zip
Claimed Product: Advanced Mac Cleaner
Detection Name: Auto.C59AC3.212256.in02

SHA 256: c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f
MD5: e2ea315d9a83e7577053f52c974f6a5a
VirusTotal:
https://www.virustotal.com/#/file/c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f/details
Typical Filename: Tempmf582901854.exe
Claimed Product: N/A
Detection Name: W32.AgentWDCR:Gen.21gn.1201

The Lifecycle of Internet Fraud: How Credit Cards are Stolen, Sold and Used for Illegal Purchases

by Ariel Ainhoren / September 11, 2018

Over the past few years, online shopping has grown significantly, making it extremely easy to order anything you like, whenever you like, to wherever you like. Technology has made it more convenient for us to purchase goods, and hackers are no exception. This why one of the most targeted sectors in the Dark Web is the retail sector. The ease in which you can commit fraud these days and get the goods delivered to your doorstep with little to no risk, is just too appealing to overlook.

A big portion of online fraud focuses on a simple 2-step process:

1. Get a stolen credit card
2. Order whatever you like with it.

From there, it's only a question of abilities and scale. Retail fraudsters range from your average neighborly hacker who uses a stolen credit card to order the new Call of Duty, to organized crime groups that buy digital goods as a money laundering tactic.

In this blog, we will demonstrate the complete lifecycle of online fraud. From stealing and selling credit cards, to stopping fraudulent transactions dead in their tracks.

Why Retail Is So Highly Targeted

Targeting the retail sector is nothing new. Fraud, scams, hacks, or plain old theft have always been challenges for shops and merchants. But with eCommerce and online shopping came cyber risks, and they are a lot riskier than their real-world counterparts.

The retail sector is highly targeted because it presents an easy target with relatively weak security, and a wide variety of companies to attack. Defrauding an online retailer is a low risk, high reward attack, and there's certainly no deficiency in credit card data available. In fact, IntSights has seen an 149% year-over-year increase in stolen credit card data for sale on the dark web. Retailers are not equipped to investigate every fraud attempt, so attackers have very little fear that the police will come knocking on their door. And most importantly, there is plenty of money to be made. Whether it's buying fancy clothes, shoes or watches to sell later, or selling dumps of credit card data, when there's an opportunity to make money, cybercriminals will flock.

How Credit Cards Are Stolen

There are a number of methods to steal credit card details. Small-time hackers obtain credit cards for their own use, while big-time players obtain cards in order to sell them on black markets to small/medium players. You can think of them as credit card wholesalers.

Here is an unexhaustive list of methods to obtain credit cards:

1. **Phishing Websites:** One of the most common ways to get credit card data is to setup a phishing website the pretends to be a legitimate online shop.
2. **Point of Sale (POS) Malware:** Infecting unsuspecting retail stores' POS machines and siphoning every credit card that's being swiped can generate hundreds to thousands of credit card numbers per day.
3. **ATM Skimmers:** Physical card readers that can copy the data of every card entered in the ATM.
4. **Malicious Apps:** Whether it's impersonating a bank's mobile app, or just keylogging credentials in a legitimate app, malicious apps are a very prolific way to get credit card and bank data.
5. **Trojan Malware:** Infecting your computer with a keylogging and screenshot-taking app that monitors your activity on your bank or credit company sites.
6. **Social Engineering:** This can be a fake bank support call line, a SMS that leads to a phishing site, a tax return request, or a fake job proposal. Social engineering is very hard to mitigate as it depends on a person's voluntary action, which is hard to anticipate and prevent.
7. **Black Markets:** Don't want to go through the hassle of the above methods or don't have the skills? Just go to a black market and buy a bunch of stolen credit cards for $1 to $20 each, depending on the quality and freshness of the card (Figure 1).

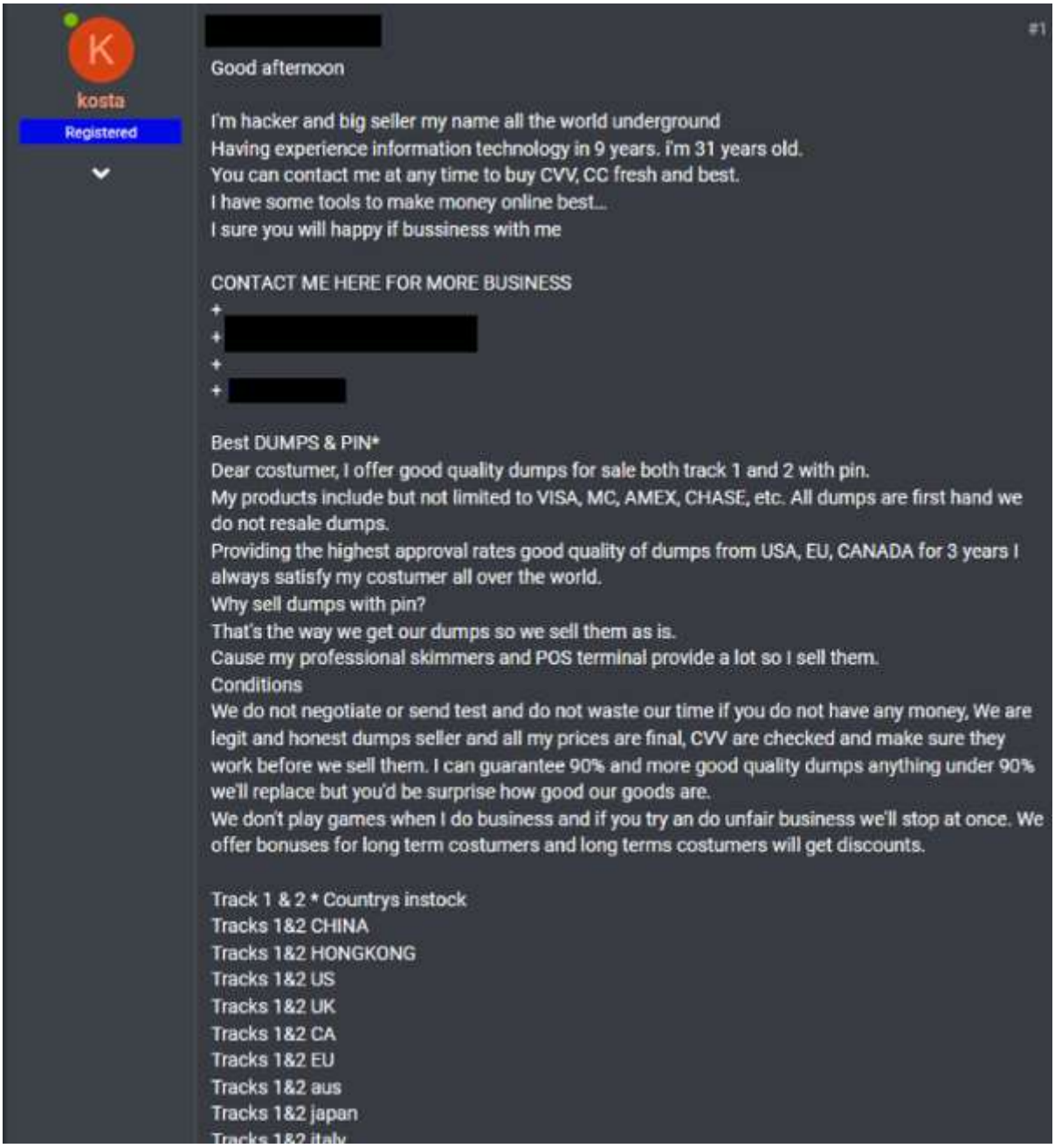

Figure 1: Black Market Credit Card Retailer

The Credit Card Life Cycle

From the moment a credit card gets stolen, it begins its travel through the wonders of the dark web. In its first step, it will usually will end up in big database file (Figure 2). That database can be used for personal use, sold as a bulk credit card dump (such as a Fresh credit card DB), or sold separately, one by one in Dark Web CC shops (Figure 3). In a CC shop, you can filter cards individually by bank, card brand, type, level, location etc.

CC shops are more profitable to the vendor, as the price per card is higher, and can also be more useful to the buyer, as they can buy cards that are specifically suited for their location or buying needs. However, buying in bulk can be cheaper for the buyer, and easier for the seller, which is why it's common to see large dumps of credit cards being sold as well.

Figure 2: Leaked Credit Card Database

Buyers can be anyone from a lower-level hacker, street-level criminal with minimal knowledge of computers, or even a neighbor kid trying to bolster his monthly allowance.

After a card has been obtained, it can be used to buy goods in the real world, or online. However, with ever-evolving defense systems, physical fraud is declining. It is less likely today that a criminal will just walk into Home Depot and try to pay with a stolen credit card. For those brave enough, the Dark Web is full of guides for how to do that, and which stores are least defended.

These days, cyber fraud is the preferred method because it's more convenient and less risky. Why risk getting caught using a stolen card at Home Depot, when you can just sit in your living room in your underwear and order an Xbox to your doorstep. If the transaction doesn't work, you can just try the next retailer.

Figure 3: Dark Web Credit Card Shop

Conclusion

eCommerce spans many different sectors and allows users to purchase goods from companies of all sizes. Whether it's clothing, technology, food, or services, the list of fraud opportunities is endless. eCommerce and online shopping has grown exponentially in recent years, and the threats grow with them. It's important to understand this lifecycle of credit card fraud so you can identify and reduce the use of stolen credit cards before they are used for fraud. Without intelligence and dark web visibility into the evolving threats around you, you'll be blind to the attacks and scams that will most certainly come your way.

Upgrade Your Threat Intelligence Program Part 3: Leverage Automation & Integrations

by Nathan Teplow / September 24, 2018

To continue our blog series on how to upgrade your threat intelligence program, we turn to part 3: **leverage automation and integrations**. The longer a threat goes unmitigated, the bigger risk it poses. That's why automation is key to an effective threat intelligence program. Using integrations and automated remediation can significantly reduce your time to mitigate threats--making your team more efficient and lowering your overall cyber risk.

Here is how organizations can leverage automation and integration to increase the overall efficiency of their threat intelligence program.

Operationalizing Your Threat Intelligence

Operationalizing your threat intelligence is a key part of a mature threat intelligence program. You may find some great solutions or services that provide you with a lot of information, some of it better than others, but you still need to have people available to take action on it. Here are some common examples of threat mitigation you can automate through integrations and policies.

Phishing Domains

Phishing is one of the most common tactics used by hackers. You may get an alert about a phishing domain or website that you want to block in your mail gateway, firewall or proxy. Having this intelligence fed directly into your security devices to automatically block that threat (instead of relying on manual blocking) will significantly reduce the incident response time. It also reduces the labor needed to manage this intelligence, which is already a scarce resource for threat intelligence teams. So any time savings you can achieve are incredibly helpful.

Threat Takedown

Another example is taking down threats on other web properties, like social media or application stores. Let's say you identify a suspicious social media page leading to a phishing site. You'll want to engage with that social media platform to initiate a takedown of that page. This process often involves your legal department or an external law firm, which can significantly extend the time it takes to remove the page. Leveraging automation and takedown partnerships can help reduce the time and effort needed to remove external threats.

Compromised Email Credentials

There are tons of credentials that are compromised every day through a variety of channels around the globe. The bigger your organization, the more credentials you have. Many employees use their work emails to sign up for various services and logins, which can complicate the identification and mitigation process. It's one thing to identify if an email address has been leaked, but you also need to know if that account is still on your network so you can determine the impact to your organization.

Integrating this intelligence with your Active Directory helps you automatically identify compromised credentials that pose a direct threat to your organization. Furthermore, if they are an active employee, you can automatically configure certain mitigation actions, like password resets, account locking or forcing a password change on the next login.

Operationalizing your threat intelligence enables you to take action quickly without your team spending cycles on repetitive tasks. Instead, they can focus on strategy and more proactive threat hunting.

Stay tuned for Part 4 coming next week. If you'd like to catch up on our previous posts in this series, you can do so here:

- Part 1: Leverage Your Digital Footprint for Context and Relevancy
- Part 2: Focus on Action, Not Searching

How Cybercriminals Use Pinterest to Run Fraud Scams

by Orin Mor / September 26, 2018

Over the past few years, we've seen a noticeable increase in cybercriminals using social media as part of their attack strategy. Whether it's a phishing campaign, online impersonation or just simply trying to promote their goods or services, social media provides hackers with a large audience that typically has their guard down when it comes to cyber scams.

One of the social media platforms that's becoming more popular among cybercriminals is Pinterest. There are a variety of scams hackers can run on Pinterest, but for this post we'll focus on fraud and financial scams.

Why Hackers Use Pinterest

Pinterest is a social media platform designed to help users share and discover information on the world wide web. It's mostly used for harmless activity, such as sharing recipes, clothing, design styles and many other items, which users can pin and save to their boards. Pinterest has become one of the most popular social media and sharing websites in the world. But where there are users, there are threat actors.

Pinterest is a great marketing tool for cybercriminals. They have a huge pool of users that they can market their goods and/or services to. In addition to the increased reach, publishing on Pinterest can give users the illusion that these activities are not necessarily illegal, for example, selling stolen products of a company using its name will not raise many suspicions.

Financial Fraud on Pinterest

There's a variety of fraud schemes and tactics that cybercriminals use, but financial fraud is one of the most direct and easiest methods. Gaining access to someone's credit card or bank account information makes it very easy to commit financial fraud, so this is often the intent we see with threat actors using Pinterest.

Money Hacking Tool

One example we saw was a "hacking tool" that claimed it could add any amount of money to your credit card (see Figure 1). All you have to do is enter the card number and select the amount you'd like to add. Sounds "phishy", right? Well it probably is; yet this is a common social engineering scheme that people fall for. While in theory the hacker might be using sophisticated carding methods to transfer money, it is most likely just a scam to collect a credit card number.

One of the obvious uses of a credit card number is for fraudulent purchases. But there's another use for credit card numbers as well.

Many banking and financial sites use a credit card number as an authentication method to login to sites and/or verify an identity. If a threat actor gets a group of credit card numbers (like using the tool in Figure 1), they now have access to a pool of user names, and just need the password to log into their accounts. This can be done through brute force or looking at other compromised credentials, as users typically use weak or similar passwords.

Once hackers have access to someone's account, not only can they commit fraud, but they can steal other personal information as well. Just recently we have seen several banks in North America that faced severe damage from these types of scams, where hackers stole users' credit card credentials, which were later used to steal personal information from the banks' portals.

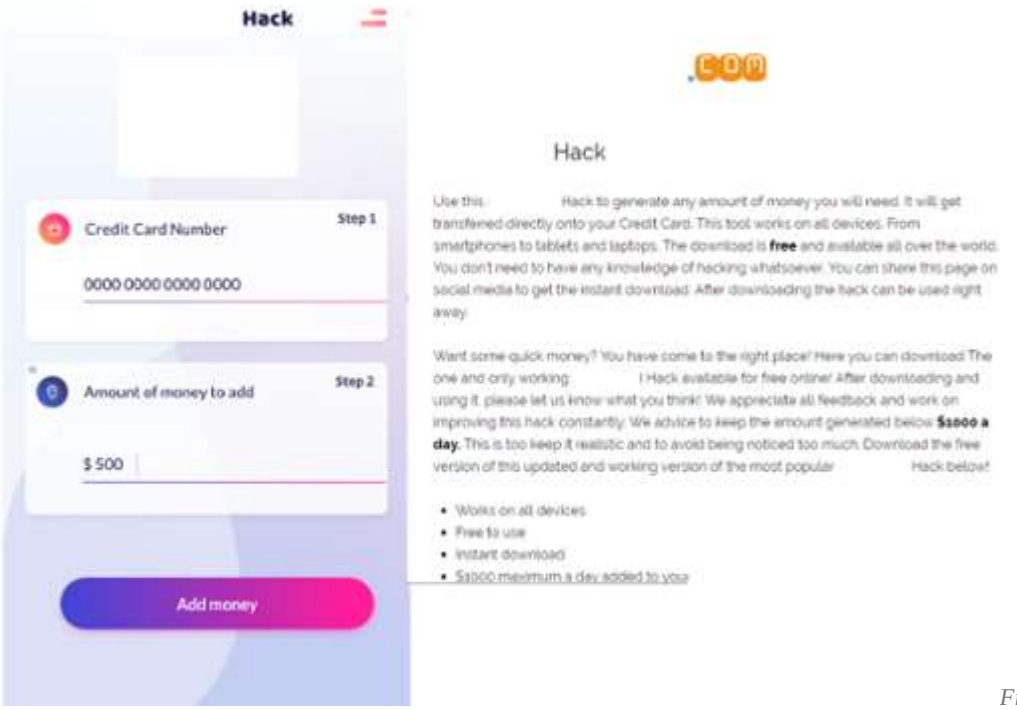

Figure 1: Example of Credit Card Hacking Tool

Fake Bank Statements

Another example we came across were posts for creating a fake bank statement. People often need to produce bank statements for demonstrating their financial stability, and they might look to forge these documents to get access to better rates or loans. As you might expect, when there's a need for illegal services, cyber threat actors are there to provide one, yet often with a caveat.

Figure 2 is an example of a bank statement template advertised on Pinterest. Obviously, this poses a threat to banks and financial institutions, who risk being duped by fake statements. However, this is more risky for the user, as the threat actor who designed the template is almost always collecting the information submitted on their end. So when a user inputs their bank data to create a fake statement, the hacker is getting all of that data, which they can use in the future for highly tailored phishing attacks.

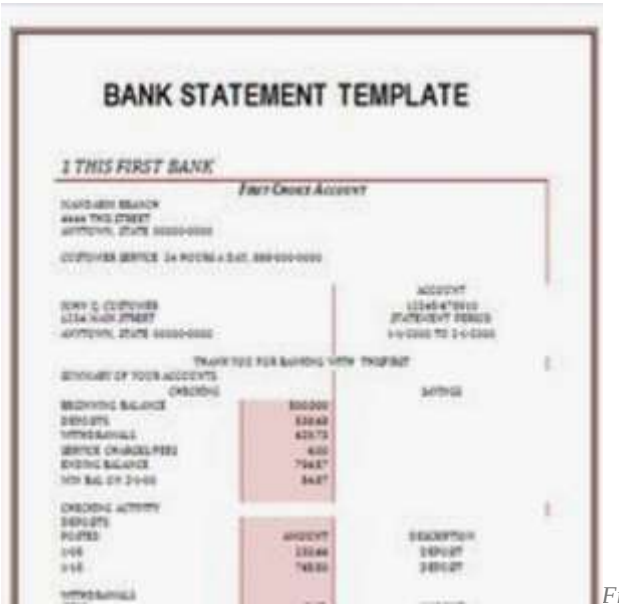

Figure 2: Bank Statement Template Found on Pinterest

Fake Pinterest Accounts

Another tactic we observed is the use of fake accounts, which pose a threat to your brand reputation and to your customers, often those that are most loyal. These fake accounts can fool users into giving away sensitive information that can be used for financial fraud.

Even though user awareness for phishing has grown over the past few years, hackers always try to find new ways to phish information, and one of the latest methods we're seeing is through brand impersonation on social media. When users are on a platform they're familiar with, like Pinterest, they usually have their guard down, which makes them more susceptible to phishing attacks.

It can be difficult to spot a fake profile on Pinterest, so users should be aware of some key characteristics to look for. First, make sure to consider the number of followers. A low number of followers for a popular brand is usually an indication that it may be a suspicious page. In addition, look at how long the page has been in existence and what other information or posts the page has shared.

Here are some more good tips on how to spot fake social media accounts.

Conclusion

In the past, cybercriminals kept most of their campaigns on the dark web, where they had access to other cybercriminals and were less likely to get caught. But to reach new audiences, they've needed to expand, and social media is one of the places they've turned to. Whether it's impersonating a brand to phish customer information, or just trying to spread the word on a new fraud tool (like a fake bank account generator), social media provides access to a large pool of users who typically are less aware of cyber scams. While social media poses a higher risk of getting caught compared to a dark web forum, it appears to be worth the risk, as we've seen more and more cyber scams and fraud campaigns make their way onto social media.

Just like with any social media site, users should be aware of these common tactics so that they can use these platforms safely. In addition, threat intelligence teams must monitor these platforms for fake accounts or suspicious tools so that they can take down malicious posts and protect their users.

