THE NEW CRIMINAL TOOLBOX

TOOLS AND TACTICS FOR MODERN CRIMEWARE

AUGUST 2019

This Report is licensed by NuData Security,
a Mastercard company.

NuData Security
mastercard

Javelin Advisory Services
Retail Banking

javelinstrategy.com | 925.225.9100

JAVELIN

TABLE OF CONTENTS

TABLE OF FIGURES

ABOUT JAVELIN: Javelin Strategy & Research, a Greenwich Associates LLC company, provides strategic insights into customer transactions, increasing sustainable profits for financial institutions, government, payments companies, merchants and technology providers.

AUDIENCE: Identity protection service providers, financial institutions, credit card issuers, investment firms, and government regulatory agencies.

AUTHOR: Kyle Marchini, Senior Analyst, Fraud Management

CONTRIBUTORS: James Lee, Analyst, Digital Banking
Crystal Mendoza, Production Manager

EDITOR: Craig Lancaster

PUBLICATION DATE: August 2019

OVERVIEW

The growth of fraud over the past decade has fueled the rise of a sophisticated criminal economy. Individuals getting started in fraud, or existing teams changing their focus, rarely need to build their own tools, instead turning to marketplaces that offer nearly any program or service they desire off-the-shelf. The availability of sophisticated data stealing and emulation/spoofing tools mean that the baseline level of skill for attacks on banks, merchants, and any other organization holding valuable data continues to rise.

PRIMARY QUESTIONS

- What types of tools cybercriminals have available off the shelf to steal victims' data while concealing their own identity.
- How tools like trojans, emulation, and formjacking have evolved to keep pace with anti-fraud technology.
- How financial institutions should adapt their fraud controls to address current and emerging threats.

EXECUTIVE SUMMARY

KEY FINDINGS

Mobile malware is a threat to the U.S., but infection pathways are still limited. Unlike with malware that targets laptop and desktop computers, smartphones typically require users to actively consent to install new software, including malware. This limits mobile malware to three main distribution pathways: phishing/smishing, unofficial app distribution, and beating malware detection measures at major app stores.

Overlays represent the next generation of phishing schemes. Overlay attacks insert a malicious window over the app opened by the victim and request that the user enter login credentials, payment information, or other information targeted by the malware operator. Because these windows are tailored to match the design of the targeted app's interface and users already believe they are entering a trusted environment, these attacks co-opt unwitting users' trust to persuade them to enter information.

Phishing schemes are evolving along with authentication methods. From overlay attacks prompting users to capture images of their ID documents to dynamic phishing pages that update to capture second authentication factors, criminal tools have adapted to capture the most prevalent authenticators used in the U.S. today.

Emulation tools now clone legitimate digital fingerprints. Unlike earlier tools that just provided fraudsters with clean digital profiles, criminal stores like Genesis Marketplace offer digital profiles captured from infected devices, often including credentials associated with that device.

Online and mobile banking trojans can piggyback on legitimate sessions to initiate fraudulent payments. For online banking trojans, this requires intercepting and modifying payment information as users enter it in their online banking sessions. For mobile banking trojans, the process is somewhat more complex, requiring abuse of accessibility services to emulate touch interaction with the smartphone screen, but at least one mobile trojan has been observed initiating fraudulent transfers after victims authenticate into their PayPal app.

The breadth of criminal tools has enabled fraudsters to economically seek out new targets. Every industry is in digital transformation, so many of the tools and tactics fraudsters have used to compromise accounts at financial institutions are used to take over accounts at merchants, mobile networks, and fintech tools like person-to-person (P2P) payment services.

RECOMMENDATIONS

Prepare for the end of one-time passwords. Whether delivered through SMS, email, call, or app, one-time passwords show their vulnerability to online and mobile banking trojans. Fortunately, protocols like WebAuthn are laying the groundwork for strong device authentication and moving biometrics to online banking. While it will still be several years before these capabilities reach maturity and acceptance among consumers, by binding a strong authenticator to a specific device and that device to the banking session, these authentication methods are much more resilient than one-time passwords or knowledge-based authentication (KBA) against the types of crimeware in use today.

Watch out for document capture replays. When document scanning at account opening or for step-up authentication is used, pictures taken from within the mobile app are more reliable than image files submitted by the user. Financial institutions should review the anti-replay methods in place with vendors that are used for document capture and verification.

Use behavioral analytics to monitor for anomalous activity. Changes in user behavior between or within sessions can indicate malware piggybacking on legitimate users' sessions. Due to the latency inherent in remote access to a user's device, behavioral analytics and biometrics are especially well suited to detecting remote-access trojans and automated attacks.

Use transaction signing/responsive alerts to combat in-session data modification. When users initiate a payment to a new recipient within online or mobile banking, they should receive an out-of-band alert containing the payment amount and recipient that they can compare with the information on their screen. In cases deemed particularly high-risk, users can be required to confirm the transaction information through a secondary channel, such as a push notification through their mobile banking app.

Alert users to suspicious login attempts. Notifying account holders when a suspicious device attempts to log into their account not only can prevent legitimate customers from being locked out if the attempt was wrongly flagged but also can prompt them to take additional measures, such as changing their password or enrolling in two-factor authentication (2FA), if the login attempt was fraudulent. Additionally, providing a portal where account holders can view recent devices associated with their account enables users to address suspicious activity that made it through their account controls. They can also decommission legitimate devices that will no longer access the account.

Educate consumers about best practices in mobile security. Although app security and authentication can mitigate the damage caused by malware, infections can be effectively prevented only by encouraging users to engage in secure practices. Key areas for education include:

- *The risks associated with sideloading:* Third-party app stores frequently lack the formal vetting conducted by official stores like Apple's App Store. Loading unofficial versions of apps exposes users to an elevated risk of malware infection. When third-party Android package kits (APKs) must be loaded onto a device, users should immediately revoke permission to install untrusted apps to prevent malicious apps from being surreptitiously placed on the device.
- *Identifying risky apps from legitimate sources:* Even when installing apps from legitimate stores, users should be cautioned to avoid apps with few downloads and reviews. Additionally, users should check that the permissions requested by the app match the expected feature set. Excessive permissions can indicate that the app has malicious functionality.
- *Best practices for securing mobile devices:* Android users should be encouraged to install an anti-malware service on their device. Providing recommendations of a few trusted providers can help users narrow down their choices and increases the likelihood that they will follow through on installing such tools.

THE NEW CRIMINAL TOOLBOX

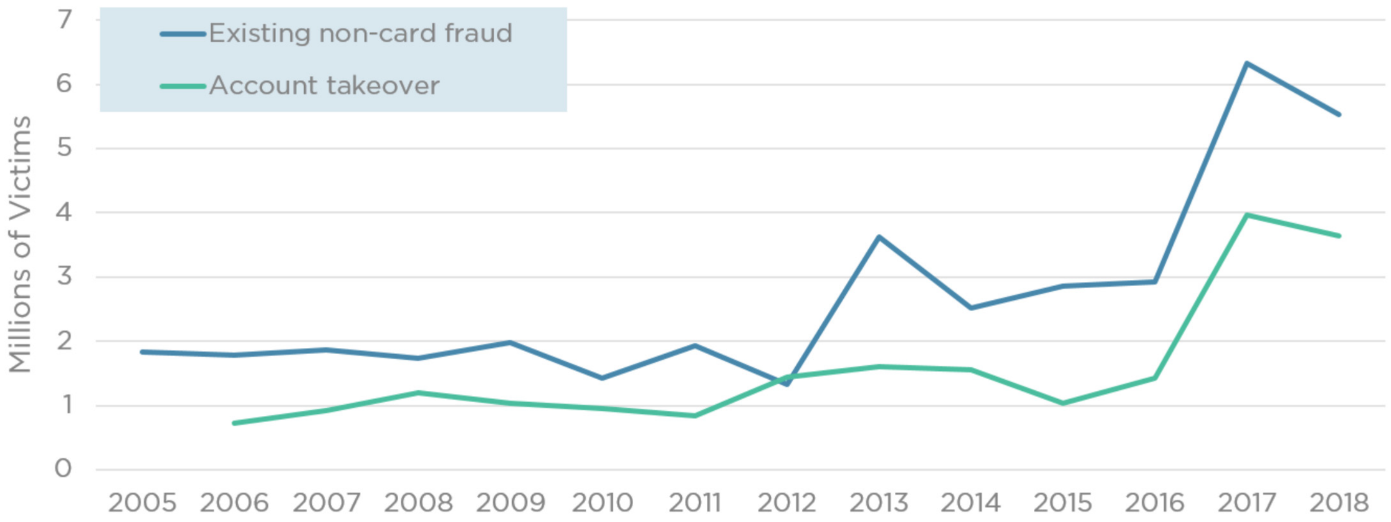
In the wake of the U.S. transition to EMV chip cards, fraudsters were forced to dramatically change their business model. Rather than using data collected through skimmers and infected point-of-sale (POS) systems to clone physical magnetic-stripe cards, fraudsters had to turn their attentions to remotely compromising accounts.

For fraud rings specializing in counterfeit-card fraud, the transition to digital fraud is not necessarily straightforward. POS card fraud required hardware for encoding blank cards with stolen Track-2 data that was either compromised with physical skimmers or frequently bought in bulk from hackers who infected POS terminals with malware. Avoiding detection required maintaining networks of runners who relied on knowledge of local merchants to reduce the risk of repeatedly encountering the same staffers while making fraudulent purchases.

In contrast, even for simpler digital fraud schemes, such as the use of stolen card data to make purchases online, fraudsters need to conceal their device and location to avoid being detected by even rudimentary IP or device-based anti-fraud tools. But with the widespread availability of more refined criminal tools, attacks with greater sophistication are on the rise. In 2017, account takeover and compromise of non-card accounts spiked as fraudsters shifted their attention fully to targeting digital portals. While the incidence of both fraud types dropped off slightly in 2018, they remain at more than twice their historical rates. Successfully compromising digital accounts requires a complex attack chain that begins with a phishing email or malware infection and usually ends with a mule transferring stolen funds to the fraudster.

The Shift to Digital Fraud Requires New Tools and Tactics

Figure 1. Millions of Victims of Existing Non-Card Fraud, Account Takeover (2005-2018)



Source: Javelin Strategy & Research, 2019

As more fraud rings have targeted online accounts, the tools they use have become commoditized. Many groups that previously designed malware and other toolkits for their own use have shifted their business model and become the arms dealers supplying newer fraudsters who lack the technical skills to build their own toolkits. In turn, newcomers aiming to get started in fraud and cybercrime have access to an immense catalog of tools available on legitimate and criminal marketplaces.

For financial institutions, digital wallets, and fintech providers, this means the baseline for combatting fraud keeps getting higher. The widespread availability of criminal tools makes it comparatively straightforward to impersonate trusted brands, steal a variety of consumer data, and conceal activities from rudimentary anti-fraud measures. This makes it imperative that financial institutions, and anyone supporting payments, understand the nature of fraudsters' tools and how they are used to circumvent defenses.

WHAT IS CRIMEWARE?

When we refer to "crimeware," we are referring to off-the-shelf tools available to criminal organizations to promote their fraud schemes. Broadly speaking, these tools can be categorized to the stage of fraud where they are used:

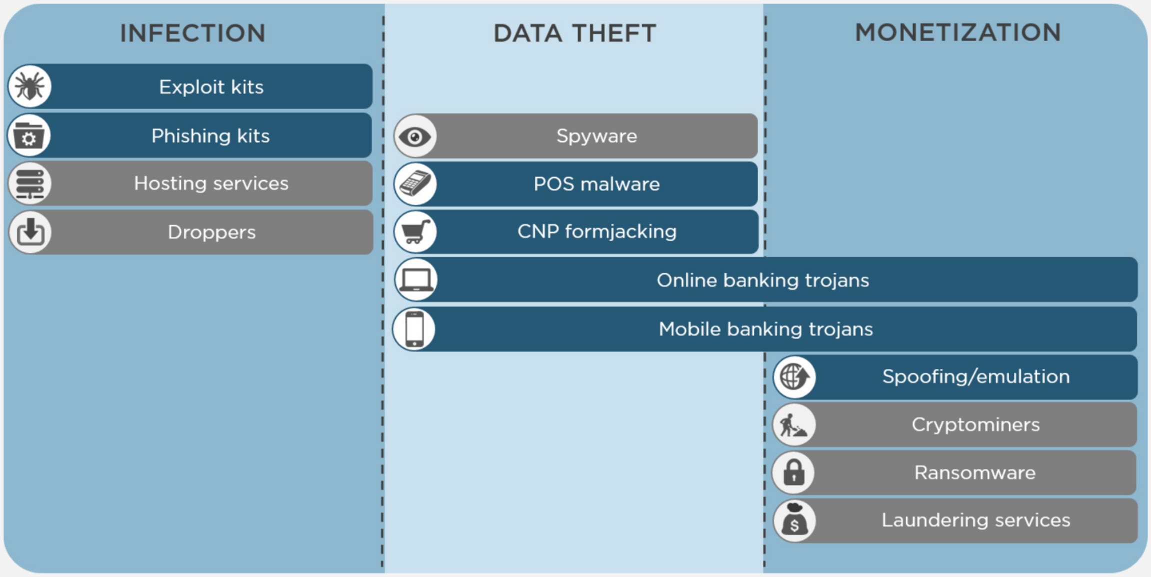
- **Infection:** In the early stages of an attack, fraudsters aim to gain a foothold on a new device or network. Frequently, this starts with a phishing email or a visit to a website compromised by an exploit kit.
- **Data theft:** With access to a device or network, fraudsters seek access to data useful to their fraud schemes. This includes obvious targets like usernames, passwords, and card data, but also less-intuitive targets like browser cookies and contact lists.
- **Monetization:** Ultimately, fraudsters make money through unauthorized transactions and transfers out of victims' accounts. This category includes tools designed to conceal fraudsters' activity as they move funds out of accounts as well as automated tools that let them piggyback on legitimate banking sessions.

With relatively mature criminal markets, fraudsters do not need to complete this entire process on their own. Many rings will jump straight to the final stage, buying stolen credentials in bulk from other groups that were able to exfiltrate the information from compromised devices. Even malware operators will contract with groups that achieved the initial infection and now sell the ability to install malware through their dropper services.

In this report, we will exclusively cover crimeware tools used in the attack chain leading up to fraud (highlighted in blue in Figure 2), but numerous other services are available to fraudsters and other cybercriminals as potential revenue streams. Adware, cryptominers, and ransomware are three of the most prevalent methods for cybercriminals to directly monetize an infected device.

Growing Toolset Facilitates More Sophisticated Fraud

Figure 2. Key Types of Crimeware



Source: Javelin Strategy & Research, 2019

IDENTIFYING VICTIMS

Every heist starts somewhere, and for fraud that typically means gaining a foothold on a consumer or corporate device to plant data-stealing malware or social engineer victims into providing their own information to the fraudster.

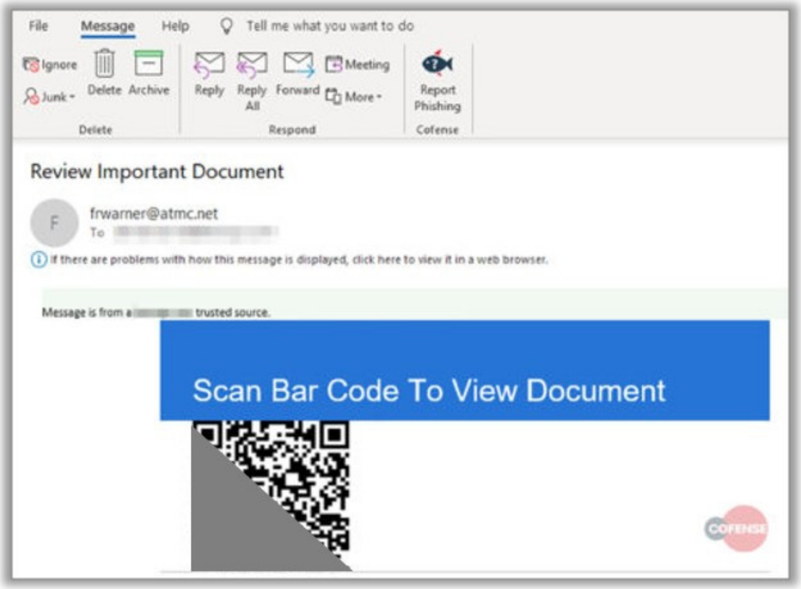
SPAM/PHISHING KITS

Phishing kits are packages used to create imitation webpages that deceive users into believing they are entering their login credentials or personal information into a trusted site, such as their bank, merchant account, email provider, or enterprise tool. Because of the short life expectancy of a phishing site—most can be expected to last only for a few days before being rendered ineffective by a takedown or automated blocking—phishing kits are one of the most commoditized parts of the crimeware market. These packages are available at a variety of prices and levels of sophistication, depending on the buyer's needs and budget. However, particularly stingy buyers will find that there is no such thing as a free lunch; free phishing kits frequently have backdoors built in that allow the creator to siphon off the data captured during the campaign.

Frequently, a phishing kit will include the full package of everything fraudsters need to clone a specific site, including HTML, CSS, and image files, along with the back-end code to capture credentials entered into the site and send them in a manageable format to the operator of the phishing ring. Alternately, fraudsters can acquire do-it-yourself kits that let them create their own phishing pages, mimicking any site they choose. This can

QR Code Phishing Bypasses Corporate Controls

Figure 3. QR Code Phishing Email Sample



Review Important Document

frwarner@atmc.net
To [redacted]

If there are problems with how this message is displayed, click here to view it in a web browser.

Message is from a [redacted] trusted source.

Scan Bar Code To View Document

Image source: Cofense[1]

extend the life expectancy of the kit by enabling fraudsters to put up new sites once old ones become ineffective or they begin a new spam campaign.

In a particularly interesting new development, one kit used QR codes embedded within the phishing email. When scanned on the victim's smartphone, the URLs directed the user to a malicious SharePoint lookalike page intended to capture their Microsoft, AOL, or other credentials. Without an actual URL included within the text of the email, this phishing scheme manages to evade URL-based anti-phishing tools. Additionally, by effectively jumping from the target's laptop to smartphone, the operator of the phishing kit aims to circumvent enterprise security tools like web content filters and secure email gateways.

While most phishing kits are static in that they simply generate the page from the files and templates included within the kit, fraudsters can also make use of remote proxies to dynamically update phishing pages, passing user information along to the legitimate target site and updating the phishing page to request more information if enhanced authentication is required. This type of attack was demonstrated by the Modlishka tool, developed by Polish researcher and penetration tester Piotr Duszyński.[2] With this type of tactic, everything the user sees within a browser is pulled from the legitimate site but is intercepted and monitored by the phishing server. Dynamically pulling information from the target page has the advantage of being able to capture time-sensitive authenticators, like one-time passwords, but also increases the risk of exposure as a web analytics tool in place at the targeted organization may detect repeated automated attempts to access the organization's page.

EXPLOIT KITS

In addition to phishing emails, cybercriminals will use exploit kits embedded in compromised websites or advertising networks to infect victim devices. Exploit kits are packages of malicious code that scan devices they encounter for software with known vulnerabilities, frequently outdated browsers or common tools like Flash that allow them to target the widest possible array of devices.

When a user visits a compromised site, the exploit kit scans the device for software with exploitable vulnerabilities. If a vulnerability is available, the kit will attempt to use it to download whatever piece of malicious software the operator is distributing. While some exploit kits, such as the now-defunct Angler, have used zero-day exploits, many use years-old vulnerabilities, relying on the persistent use of outdated and unpatched software to maintain their infection rate.

Exploit kits have one distinct advantage over phishing kits in that they do not require users to directly interact with the compromised content beyond simply navigating to the page. Embedding exploit kits in compromised advertising networks can allow fraudsters to hit multiple targets more economically than if they were forced to individually compromise each targeted website. Today, exploit kits have taken a second seat to phishing as a means of distributing malware after the takedowns of high-profile kits like Angler. Additionally, the use of comparatively more hardened browsers like Chrome and Firefox rather than vulnerable browsers like Internet Explorer have reduced the opportunity for exploit kits to infect victims in the U.S.

MACRO BUILDERS

Since most users—and anti-virus programs—are suspicious of executable files arriving through email, even from an apparently reputable source, weaponized Microsoft Office files are one of the most popular means of converting a successful phishing email into a malware infection. With these files, fraudsters embed malicious functionality into a macro within a Word or Excel file, which downloads the actual malware once the macro is run.

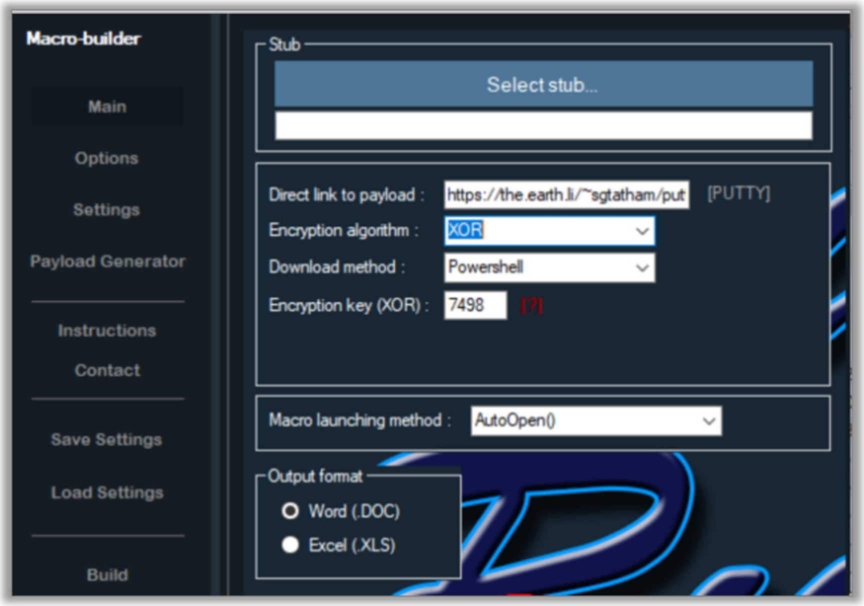
Fraudsters typically rely on social-engineering attacks to overcome integrated security features that prevent macros from running without active user permission. Frequently, the weaponized document is presented as an invoice, a time-sensitive notice, or some other critical document marked as being protected against access from unauthorized users. To access the document, so users are told, they must download the file and click "enable content," which allows the macro to run and install the actual malware.

Fraudsters have plenty of tools to automate the creation of infected Office files. One example is the Rubella macro builder, available to license from $120 per month and whose suspected operator was arrested earlier this month. This service enables phishers to automate the creation of malicious Office documents by providing a link to the payload and specifying the type of file they would like to create and a few other parameters, such as the encryption algorithm and key.

Frequently, this initial payload will just be a "dropper"—a piece of malware that does little on its own but enables the malware operators to subsequently install additional malware on the infected device. This gives the malware operator quite a bit of versatility in monetizing the infected device, whether through a direct monetization scheme like ransomware or adware or the longer process of compromising credentials and targeting the victim's financial accounts.

Macro Builders Automate the Creation of Malicious Office Documents

Figure 4. Rubella Macro Builder Screenshot



Direct link to payload : https://the.earth.li/~sgtatham/put [PUTTY]
Encryption algorithm : XOR
Download method : Powershell
Encryption key (XOR) : 7498 [?]

Macro launching method : AutoOpen()

Output format
○ Word (.DOC)
● Excel (.XLS)

Image source: Flashpoint[3]

COMPROMISING CUSTOMER DATA

If the cybercriminal intends to make use of the compromised device to perpetrate fraud, the typical next step is to siphon specific types of data from the device. The particular data targeted will depend on the type of device and the end goal of the fraudster. Login credentials, step-up authentication responses, card data, and sensitive Personally Identifiable Information (PII), such as Social Security numbers, make for obvious targets, but fraudsters will also frequently target less-conventional data like browser cookies and contact lists, which can improve their odds of success as they attempt to drain victim accounts or can provide a secondary revenue stream through sale to other cybercriminals.

ONLINE BANKING TROJANS

These date almost to the advent of online banking. The Zeus banking trojan was first uncovered in 2006 but still has relevant functionality today. The hallmark of a banking trojan is the use of injection techniques to intrude on users' browsing sessions, intercepting data as it is being entered or modifying data before it is transmitted to the recipient server.

Typically, online trojans operate by hooking functions within the browser responsible for processing HTTP requests prior to encryption or following decryption. This allows the malware to monitor for victims' attempts to navigate to a targeted webpage and redirect the user to a phishing site without the victim having a chance to notice anything suspicious. By dynamically updating the phishing page as the victim enters their information, modern online banking trojans can steal and immediately use any data entered by the user into an online banking page, including security questions and one-time passcodes.

In other cases, the malware will directly inject malicious javascript into the browser through the developer window or by entering it into the browser bar. To address this type of tactic, when users paste a string beginning with "javascript:" into the navigation bar, major browsers will remove the "javascript:" prefix, requiring the user to manually retype it. The BackSwap malware family addresses this countermeasure by emulating the user typing the prefix in individual keystrokes, rather than by copying and pasting.

Notably, most modern online banking trojans are built as modular programs, which allow the operator to add additional capabilities as they become relevant. Typically, these modules add functionality complementary to the primary goal of perpetrating fraud and generally include canvassing infected computers for stored data that increase the ease of infecting other devices or improve the odds of successfully cashing out the victim's accounts. Types of ancillary data targeted by banking trojans can include:

- Stored cookies: Capturing cookies from a user's device can help fraudsters more successfully impersonate the user during later interactions with webpages that rely on these cookies to identify returning visitors.
- Contact lists: Exfiltrating email contact lists can be used by the fraud ring or sold to other organizations that compile spam mailing lists. For more specific spear-phishing campaigns, identifying frequent contacts can help fraudsters craft targeted messages aimed at linked individuals, thus improving the odds that the recipient opens a malicious attachment or link.
- Network credentials: Using open-source hacking tools like Mimikatz, trojans search for credentials that allow lateral movement to infect devices across a corporate network. In some cases, as with the Qakbot malware family,

the malware may attempt to brute-force network passwords to spread, potentially resulting in locking users out from corporate networks after repeated unsuccessful authentication attempts.[4]

MOBILE BANKING TROJANS

Originally, mobile banking Trojans were extensions of online banking malware. With “ZeuS in the Mobile,” or ZitMo, once a laptop or desktop computer was infected, the user would be prompted to install a new “security certificate” on his or her mobile device to ensure that the mobile banking services could operate properly. Unsurprisingly, this certificate turned out to be malware capable of intercepting and forwarding SMS messages to enable the malware operators to capture one-time passcodes and alerts sent by the victim’s bank. Today, mobile malware is more frequently a standalone program, but SMS capture has remained a core feature.

Distribution/infection pathways:

Fortunately, consumers in the U.S. are relatively better protected against mobile malware by default on Android and iOS devices than they are against malware on laptop or desktop computers. This is thanks to curated app stores that screen for potentially malicious programs. To successfully infect users, fraudsters must successfully deceive users into disabling default restrictions on installing apps from third-party sources. Frequently, this is accomplished with the same social-engineering tactics malware distributors use to get desktop users to enable macros or run an executable file: by imitating trusted sources such as the users’ bank, imbuing their message with a sense of urgency, or just appealing to users’ curiosity.

In regions of the world where users routinely install apps from unofficial stores, fraudsters have a much easier time because users are inured to warnings about the unofficial apps or will have disabled restrictions on app installations. This is much more common in parts of Asia where consumers will distribute translated versions of apps because the official app does not support the local language. In other cases, when an app gains a significant following but is available on only one operating system, unofficial ports for other operating systems will be shared outside major app stores. With less oversight in unofficial marketplaces, these apps frequently have malicious functionality. For instance, in 2017, when Super Mario Run was released solely on iOS, Android versions of the app embedded with the Marcher banking trojan quickly appeared on third-party sharing sites.[5]

The other path to infecting users is to successfully infiltrate legitimate app stores like Google Play. Despite the screening conducted by Apple and Google, every year a handful of malicious programs manage to successfully masquerade as legitimate programs and make their way into the marketplaces. In 2017, there were three incidents where the BankBot trojan was able to infiltrate the Google Play store. More recently, the Agent Smith adware was able to infect approximately 25 million devices, with most of the infections occurring in India and surrounding countries. The malware operators were able to plant infected apps in an unofficial app store popular in the region. However, around 300,000 devices were also infected in the U.S. after 11 infected apps were able to bypass the security screening in place at the Google Play store.[6]

Key functionality:

Abuse of accessibility services: In addition to the more restricted infection pathways, the other reason mobile malware has been less of a threat than malware targeting laptop and desktop computers is that it is generally much more difficult for mobile apps to directly interact with each other and observe users’ interactions with other apps. For instance, while keylogging has been a core piece of desktop malware functionality for a long time, true keylogging—detecting keystrokes as they are entered rather than capturing them through a phishing window—has only recently appeared in mobile banking trojans.

To directly interact with other apps on the infected device, mobile malware requires permission to use accessibility features, a set of tools built into mobile apps to assist users with disabilities. These tools allow an app to view other apps' screens, emulate touch input into the device, lock the screen, and offer access to a variety of other capabilities. Not only do accessibility services permissions enable features like overlay attacks, but they also allow the malware to impede attempts at uninstalling the unwanted program.

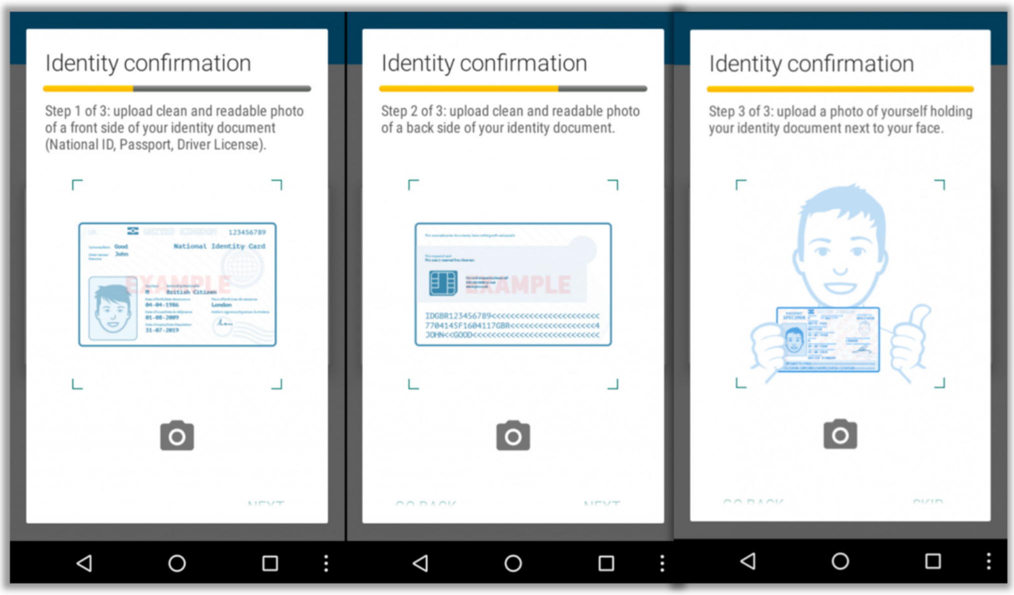
SMS interception: SMS one-time passwords are far and away the most widely used step-up authentication method among U.S. financial institutions, though with the limited mobile malware distribution pathways in the U.S., SIM swap attacks tend to be the more typical method for compromising SMS one-time passwords.

Overlay attacks: With their versatility, overlay attacks are the primary data-stealing feature for mobile banking trojans. In this type of attack, the malware monitors for the user to open a targeted app—frequently mobile banking apps, but also payments and commerce apps—and inserts a phishing screen designed to look identical to the app environment the user is about to enter.

Just as with other targeted phishing attempts, because the user is already aware of entering an environment where there's an expectation of providing sensitive personal or payment information to prove identity, additional challenges are likely to be met with frustration but not suspicion. However, because the user has interacted with the mobile banking app before with no reason for suspicion, this kind of tactic is more likely to be successful than unsolicited phishing emails or texts, which consumers have been trained to greet with skepticism.

Overlay Attacks Capture Images of Users' ID Documents

Figure 5. Acecard Document Capture Phishing Overlay



Identity confirmation

Step 1 of 3: upload clean and readable photo of a front side of your identity document (National ID, Passport, Driver License).

Identity confirmation

Step 2 of 3: upload clean and readable photo of a back side of your identity document.

Identity confirmation

Step 3 of 3: upload a photo of yourself holding your identity document next to your face.

Image source: McAfee

Depended on the targeted app, this screen may ask for standard login credentials, card information, or other PII, such as the user's Social Security number. With the Acecard trojan, the standard overlays included windows prompting users to take a picture of themselves with their ID documents for reuse during document-scanning authentication attempts.

Other notable features: Some malware now displays standard keylogging functionality, using accessibility services to monitor for the location of keystrokes as the user interacts with other apps, inferring which key was struck from the location of the touch input, regardless of whether the phone is held vertically or horizontally. This offers somewhat more versatility in capturing user's inputs during interaction with other apps than do overlay attacks or previous methods of capturing entered user data, which involved taking a new screenshot every time the user entered a letter.

RETAIL ATTACKS

POS malware: While EMV is making strong inroads against counterfeit card fraud, fraudsters are still trying to eke out the last value from merchants and issuers who have failed to modernize their payments platforms. For small businesses or those in industries where the threat of fraud is light enough to not compel a renovation of payment acceptance technology, malware targeting vulnerable point-of-sale (POS) terminals can still steal magnetic-stripe card data as it is processed. Gas stations will continue to be vulnerable due to the EMV liability shift not occurring until October 2020.

The core methodology of POS malware has remained largely consistent across even newer strains. The malware monitors the memory on the POS device for strings matching the format for Track 1 and Track 2 card data, capturing them and sending the stolen data back to the command-and-control server.

Some attacks appear to be opportunistic rather than highly targeted. For example, one module of the TrickBot banking trojan scans for whether the infected device is connected to a network that includes point-of-sale terminals, although it is not clear whether the trojan is currently able to intercept card data.[7]

Formjacking: With the rise of card-not-present fraud in the post-EMV U.S., the associated rise in demand for the data necessary to support online card fraud transactions has forced fraudsters to expand their data-stealing tactics. In 2018, formjacking rose to prominence with the emergence of the Magecart threat groups. These competing threat actors compromise vulnerable services embedded within merchant sites to steal customer card information as it is input at the webpage.

By targeting add-on services, rather than individual merchant sites, these groups can economically target even very small merchants, which would not be practical to individually attack. According to some accounts, these groups have been wildly successful, with Symantec estimating that they were able to infect more than 4,800 unique websites each month throughout 2018.[8] Although the nature of supply-chain attacks like these enables hackers to compromise much smaller sites, larger organizations were not immune. Ticketmaster, British Airways, and Newegg were breached through Magecart formjacking attacks.

KEY TAKEAWAYS FOR FINANCIAL INSTITUTIONS

Prepare for strong authentication in the browser. Protocols like WebAuthn are laying the groundwork for strong device authentication and moving biometrics to online banking. By binding a strong authenticator to a specific device and that device to the banking session, these authentication methods are much more resilient than one-time passwords or knowledge-based authentication (KBA) against the types of crimeware in use today.

Strengthen device management capabilities. Notifying account holders when a suspicious device attempts to log into their account not only can prevent legitimate customers from being locked out if the attempt was wrongly flagged but also can prompt them to take additional measures, such as changing their password or enrolling in two-factor authentication (2FA), if the login attempt was fraudulent. Additionally, providing a portal where account holders can view recent devices associated with their account enables users to address suspicious activity that made it through their account controls. They can also decommission legitimate devices that will no longer access the account.

Watch out for document capture replays. When document scanning at account opening or for step-up authentication is used, pictures taken from within the mobile app are more reliable than image files submitted by the user. Financial institutions should review the anti-replay methods in place with vendors that are used for document capture and verification.

COMPROMISING AND MONETIZING ACCOUNTS

CONCEALMENT TECH

Unlike with phishing kits, trojans, and other types of malware, many of the tools fraudsters use to conceal their identities are legitimate, or at least legal, tools available on the surface web. To avoid raising red flags at financial institutions from having a single device or location access many accounts or submitting account applications in bulk, fraudsters will emulate unique device or browser profiles and use spoofing tools to conceal their location and phone number.

Device emulation: Device emulators are legal tools that are widely available on surface web marketplaces, with some available at no cost. Outside of the criminal world, these tools are frequently used by app or web developers to test software in controlled environments. A variety of browser-based emulation tools are available on the surface web, such as FraudFox, MultiLogin, and the Tenebris Linken Sphere browsers.

While consistently changing their digital profile can help fraudsters evade detection, emulating a legitimate user's profile can allow them to skate past device recognition systems, reducing the risk that they will be challenged with step-up authentication. Earlier this year, researchers at Kaspersky Labs uncovered Genesis Marketplace, which offered a browser plugin along with around 60,000 digital "fingerprints" taken from infected devices. These device profiles ranged in price from $5 to $200, commanding a higher price if they included pieces of stolen data associated with that device, such as card numbers or credential pairs.[9] The combination of digital fingerprints and credential information is especially powerful, as it gives fraudsters one of the most straightforward means of circumventing basic authentication and contextual risk assessment methods, short of using a remote access trojan to hijack the victim's actual device.

Phone/ANI spoofing: While digital channels frequently receive the most attention and investment from fraud management teams within financial institutions, fraudsters' digital toolbox is not limited to web and mobile interfaces. For more complex and lucrative fraud schemes like account takeover, fraudsters will often move between channels to seek out the most vulnerable spots in an organization's defenses. With fewer opportunities for background risk assessment tools like device reputation or behavioral analytics, call centers frequently rely on outmoded fraud defenses like knowledge-based authentication.

ANI refers to Automatic Number Identification, a protocol used to identify the source of an inbound phone call. Using a VOIP (voice over IP) line or other tactics, fraudsters can mask the true number they are calling from, replacing it with a random number or even impersonating a specific target.

ANI spoofing is something that many consumers encounter regularly, although they may not be familiar with the process. Today, scammers and telemarketing services frequently spoof the area code and first three digits of target telephone numbers, causing the call to appear as if it originated from a number located in the recipient's city and improving the odds that the target will answer compared with instances when an out-of-area or 800-number phone call is received.

While not as common in legitimate businesses as device emulation, spoofing phone numbers is also legal if it is not done for illicit financial gain or to cause harm. Consequently, there is a wide range of call and text spoofing services available in legitimate app stores, ostensibly for consumers to protect their privacy or to prank their friends.

While some generate only a randomized phone number, the most robust spoofing services available in legitimate marketplaces enable users to specify the number they wish to spoof. Additionally, some services such as SpoofCard (see Figure 6) enable the user to apply filters to mask their voice or add background noise in attempts to mitigate the effectiveness of phone printing or voice biometric authentication methods.

For fraudsters, ANI spoofing has broad utility throughout the attack chain. During the early stages of fraud, malicious actors can impersonate a trusted organization such as a bank or law enforcement to gain additional information from victims, filling in gaps in the information they were able to obtain from criminal marketplaces, or using a tech support scam tactic to deceive users into installing malware on their devices. Once the fraudster has access to the victim's credentials or PII, spoofing the victims' ANI while calling their financial institution can reduce the scrutiny that a password reset or outbound payment is subjected to.

Legally Available Tools Enable Phone Number Spoofing

Figure 6. SpoofCard Android Interface

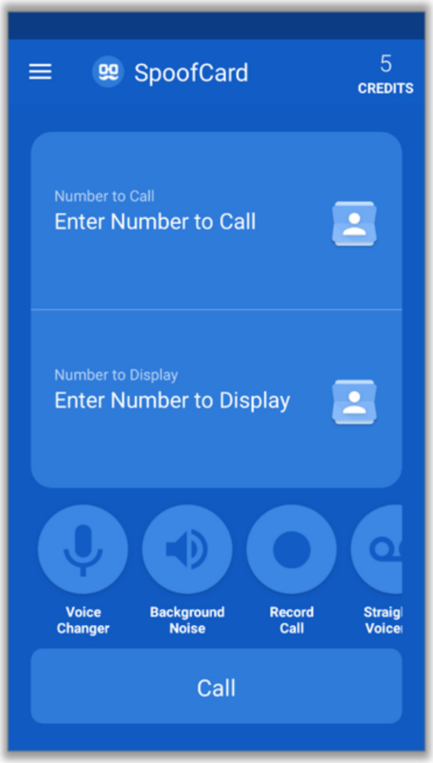


Image source: Spoofcard Android app

IN-SESSION DATA MODIFICATION

Online banking trojans: In addition to the ability to steal data entered on infected devices, some online banking trojans have features that allow malware operators to more directly siphon funds from victims.

The Backswap trojan, which targeted Polish banks in early 2018, monitors for victims to navigate to the transfer or bill payment portion of their online banking window. When the user enters the intended recipient's account number, the malware modifies the entered information to send the funds to an account controlled by the fraudsters.[10] This type of attack is somewhat less reliable, being contingent on victims initiating an ACH or wire transfer to a new recipient. However, because the victim is legitimately attempting to send an outbound transfer, he or she will be able to pass any step-up authentication attempt, including authentication methods tied to the specific device and session, like hardware security keys or other WebAuthn-based authentication methods. Additionally, unless an alert sent to notify the account holder of a new transaction includes details of the recipient of the funds and the victim is aware enough to notice the inconsistency, the victim is unlikely to discover the fraud until the intended recipient makes an inquiry about the lack of payment.

This poses an especially potent risk with the advent of real-time payments. The irrevocable nature of P2P, ACH, or wire transfers coupled with quick, cheap, and flexible money movement makes it easier for fraudsters to launder funds through multiple accounts before victims discover that the fraud occurred.

Mobile banking trojans: As with online banking trojans, some mobile banking trojans can autofill data in targeted apps, enabling the app to automate the process of stealing victims' funds. Through the abuse of accessibility features, the Gustuff mobile banking trojan uses ATS (Automatic Transfer System) to change the values of text fields in targeted banking and cryptocurrency apps.

In other cases, malware uses accessibility services to emulate touch interactions with the smartphone's screen to control apps as if the user is initiating a transfer to the fraudster-controlled account. In one malware sample targeting PayPal, once the user logs in to the app, the malware takes over the device, adds a new payee and initiates a transfer of €1000, with the currency in use depending on the location of the device.[11] Crucially, because the malware attempts to initiate and complete the transaction fast enough that the user is unable to intervene and stop the process, it results in a marked change in user behavior within the app detectable by behavioral analytics tools.

KEY TAKEAWAYS

Behavior is key to identifying anomalous activity. With advances in concealment techniques and the ability to piggyback on legitimate sessions, changes in user behavior between or within sessions can help detect otherwise stealthy fraud schemes. Due to the latency inherent in remote access to a user's device, behavioral analytics and biometrics are especially well suited to detecting remote-access trojans and automated attacks.

Alerts should move past static notification. When users initiate a payment to a new recipient within online or mobile banking, they should receive an out-of-band alert containing the payment amount and recipient that they can compare with the information on their screen. In cases deemed particularly high-risk, users can be required to confirm the transaction information through a secondary channel, such as a push notification through their mobile banking app.

METHODOLOGY

Consumer data in this report is taken from a random sample panel survey of 5,000 U.S. adults fielded in November 2018. For questions answered by all 5,000 respondents, the maximum margin of sampling error is +/-1.41 percentage points at the 95% confidence level.

ENDNOTES

1. https://cofense.com/radar-phishing-using-qr-codes-evade-url-analysis/, published June 28, 2019;accessed July 3, 2019.
2. https://www.zdnet.com/article/new-tool-automates-phishing-attacks-that-bypass-2fa/, published January 9, 2019;accessed July 22, 2019.
3. https://www.flashpoint-intel.com/blog/rubella-macro-builder/, published April 25, 2018; accessed July 24, 2019.
4. https://securityintelligence.com/qakbot-banking-trojan-causes-massive-active-directory-lockouts/, published June 2, 2017; accessed July 25, 2019.
5. https://www.zdnet.com/article/android-banking-trojan-malware-disguises-itself-as-super-mario-run/, published January 9, 2017; accessed June 27, 2019.
6. https://www.theverge.com/2019/7/10/20688885/agent-smith-android-malware-25-million-infections, published July 10, 2019; accessed July 24, 2019.
7. https://securityintelligence.com/news/brand-new-bag-trickbot-malware-adds-pos-data-collection-module/, published November 30, 2018; accessed July 25, 2019.
8. https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf, published February 2019; accessed July 3, 2019.
9. https://threatpost.com/genesis-marketplace-digital-identities/143558/, published April 9, 2019; accessed July 25, 2019.
10. https://www.welivesecurity.com/2018/05/25/backswap-malware-empty-bank-accounts/, published May 25, 2018; accessed July 25, 2019.
11. https://www.welivesecurity.com/2018/12/11/android-trojan-steals-money-paypal-accounts-2fa/, published December 11, 2018; accessed July 25, 2019.