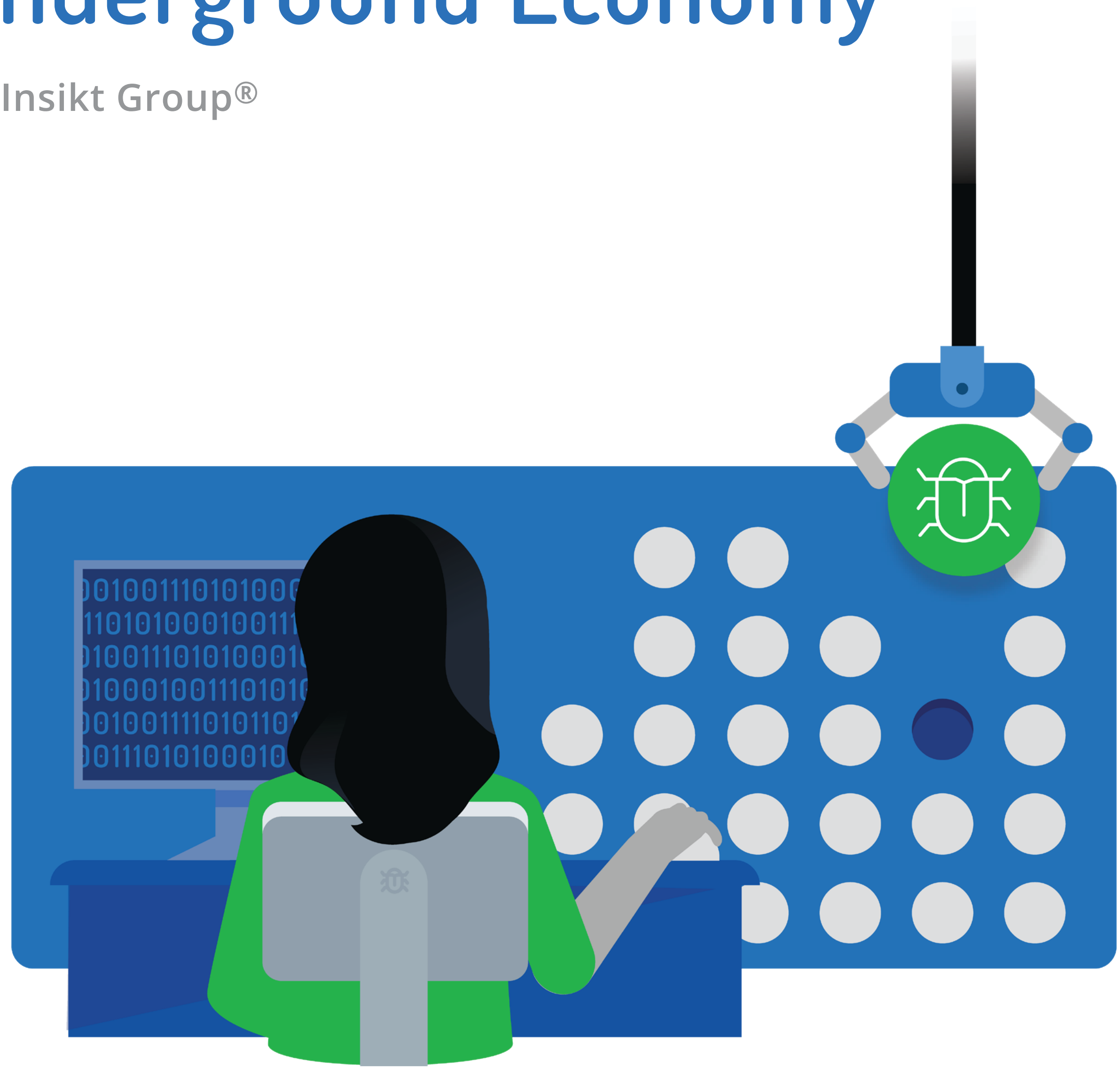
Recorded Future®

CYBER THREAT ANALYSIS

Automation and Commoditization in the Underground Economy

By Insikt Group®



CTA-2020-0324

Recorded Future analyzed current data from the Recorded Future® Platform, information security reporting, and other OSINT sources to complete this overview of 10 tools and services that facilitate threat actor campaigns. In subsequent months, Recorded Future will publish in-depth reports into each tool or service, the threat actors offering them, as well as technical details and mitigation recommendations.

"Automation" in this report refers to the removal of human interaction from repetitive tasks (such as through brute-forcers or vulnerability scanners), as well as the ability to piece together services or products that are not part of a core offering (for example, crypters, loaders, delivery methods).

This report will be of most interest to network defenders, security researchers, and executives charged with security risk management and mitigation.

Executive Summary

Automation has become an essential part of nearly every industry. Nowhere is this more true than in cybersecurity, where the scale of available data makes the automation of data collection, processing, and correlation a requisite for keeping pace with the threat landscape.

Unfortunately, the benefits of automation are also equally available to criminal enterprises. In this report, Insikt Group will describe 10 types of tools and services currently used by threat actors to automate various tasks. For each, we provide a brief overview of some notable recent developments, list some of the top vendors of these tools on the criminal underground, and provide some suggested mitigations for defenders to implement. The list is as follows:

1. Breaches and sale of databases sold on underground forums give threat actors access to accounts and credentials of clients and employees, which can be used to gain further access to internal systems or to commit fraud.
2. Checkers and brute-forcers can help threat actors to quickly and efficiently validate or access passwords for thousands of accounts.
3. Loaders and crypters allow threat actors to obfuscate and deliver malicious payloads, bypassing antivirus solutions.
4. Stealers and keyloggers allow threat actors to gather sensitive information from victim systems, including credentials, personally identifiable information (PII), payment card information, and other data.

5. Banking injects are used by threat actors as fake overlays over legitimate sites to financial institutions and similar sites where they can collect sensitive information from victims trying to visit the legitimate site.
6. Exploit kits allow threat actors to use multiple exploits simultaneously to target various vulnerabilities across different targets.
7. Spam and phishing services give threat actors access to hundreds of thousands of potential victims for their lures.
8. Bulletproof hosting services (BPHS) provide secure hosting for malicious content and activity, and assures anonymity to threat actors.
9. Sniffers infiltrate legitimate online shopping sites and collect sensitive information such as payment cards and the PII of customers from trusted online stores.
10. Automated marketplaces and logs vendors allow threat actors to sell stolen credentials and digital fingerprints to other threat actors, who use them for fraud or to facilitate further breaches, frequently circumventing anti-fraud measures.

Following this analysis, we also examine the usefulness of automation from the defender's perspective, particularly through the implementation of security orchestration, automation, and response (SOAR) solutions. SOAR solutions are able to gather together threat data and then automate repeatable incident response tasks, taking the burden away from personnel.

For SOAR solutions to work effectively, they need playbooks — repeatable, automated security workflows designed to describe threats and how to handle them. But these playbooks are only as good as the data used to construct them, and SOARs that are fed with too much external data — especially when that data is not correlated with internal network data — can't accurately assess whether an alert is malicious, resulting in delays and the possibility of malicious activity going unresolved for too long.

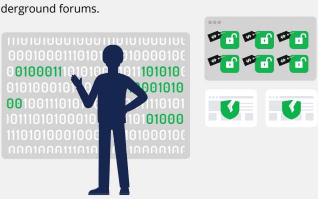
For that reason, we also outline the usefulness of threat intelligence in providing that context and data enrichment. In particular, we look at how two metrics, mean time to detection (MTtD) and mean time to response (MTtR), should be used as baseline measurements of the usefulness of automated threat intelligence over manual intelligence-gathering.

Key Judgments

- The evolution of specialization and automation on the criminal underground has created an ecosystem of tools and resources allowing threat actors to both operationalize and monetize campaigns increasingly quickly.
- Credentials are the raw materials of the underground economy. The availability of billions of credentials in the underground economy has resulted in the growth of products and services to monetize and exploit the available data in the form of checkers and brute-forcers.
- The backbone of this economy is delivery networks and botnets, which are facilitated through the use of loaders, crypters, no-distribute services, and bulletproof hosters, and are propagated through combinations of exploit kits and spam.
- Threat actors have developed flexible business models for credit card sniffers that include technical support and profit sharing, decreasing the barrier to entry into this type of cybercrime.
- Automated marketplaces allow threat actors to monetize the immense amounts of data and victims that would otherwise be impossible to sort and sell manually.
- SOCs and incident response teams that lack data enrichment provided by threat intelligence are likely to continue to struggle against increasingly automated attacks.
- SOARs can be used to tip the balance back in the defender’s favor by automating defensive intelligence feeds and combining them with automated detection and prevention to lower the mean time to detection (MTtD) and mean time to response (MTtR).

Breaches and Sales of Databases

Cyberattacks ultimately start with a compromised network or database of credentials as a result of threat actors who obtain unauthorized access to a network and then sell credentials on underground forums.



MITIGATION STRATEGIES

- Keep all software and applications up to date and story system backups offline
- Filter emails for spam and scrutinize links and attachments
- Compartmentalize or encrypt company-sensitive data
- Institute role-based access

Checkers and Brute-Forcers

These are used to direct large-scale automated login requests to determine the validity of victims or gain unauthorized access through a credential stuffing attack.

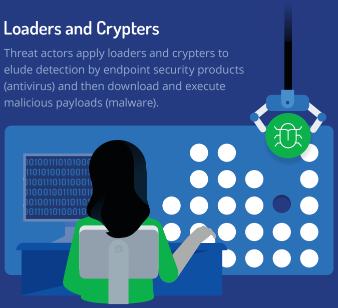
Checkers are automated tools used to check the validity of ID/password combinations.

Brute-forcers are automated password-cracking tools that can be used to discover hidden pages and content in web applications.

- Use password manager with unique passwords for all accounts
- Require CAPTCHA or MFA
- Establish customized web application firewalls
- Baseline traffic and slow down login traffic with rate-limits
- Remove unused public-facing logins

Loaders and Crypters

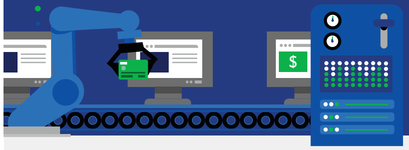
Threat actors apply loaders and crypters to elude detection by endpoint security products (antivirus) and then download and execute malicious payloads (malware).



- Update antivirus software regularly
- Implement additional response and detection controls beyond antivirus to detect malicious payload
- Educate individuals on phishing and associated risks

Stealers and Keyloggers

These are used to exfiltrate sensitive information from victims, including credentials, PII, and payment card information, and install secondary payloads onto victims' systems.



- Invest in solutions offering patch posture reporting
- Configure network defense mechanisms to alert on malicious activity on devices
- Monitor for suspicious changes to file drives and registries

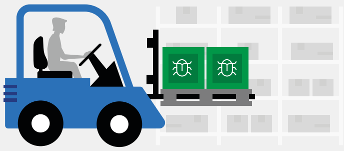
Banking Injects

Fake overlays or modules are typically used with banking trojans to inject HTML or JavaScript code to collect sensitive information before redirecting to a legitimate website.

- Keep software and applications up to date
- Install antivirus solutions, schedule updates, and monitor statuses
- Enable MFA via SMS or authenticator applications
- Use HTTPS connection
- Educate employees and conduct training sessions
- Deploy spam and web filters
- Encrypt all sensitive company information
- Disable HTML or convert HTML email into text-only email

Exploit Kits

Toolkits can automate the exploitation of web browser vulnerabilities to maximize the delivery of trojans, loaders, ransomware, and other malicious software.



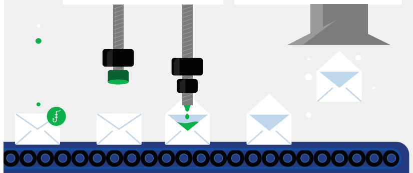
- Prioritize patching of Microsoft products and older vulnerabilities in the technology stack
- Ensure Adobe Flash Player is automatically disabled in browser settings
- Conduct and maintain phishing security awareness

Spam and Phishing Services

Fraudulent email campaigns can give threat actors access to hundreds of thousands of victims to deploy malware or gain further access into a network.

Spamming targets thousands of victims at the same time indiscriminately.

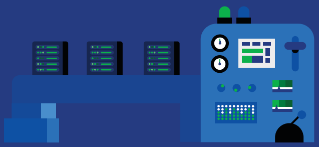
Phishing uses social engineering tactics, emulating emails from trusted or legitimate entities.



- Refrain from publishing your email address
- Do not reply to spam messages
- Download additional spam filtering tools and antivirus software
- Avoid using personal or business email addresses when registering online
- Develop a password security policy and require encryption
- Educate employees and conduct training sessions

Bulletproof Hosting (BPHS)

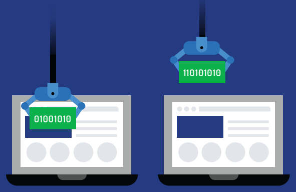
BPHS provides secure, anonymous hosting for malicious content and activity, relying on a model that promises not to comply with legal requests that would disrupt operations or result in arrests.



- Leverage threat intelligence platforms like Recorded Future to assist in monitoring of malicious service providers
- Blacklist servers affiliated with known-malicious BPHS's

Sniffers

Sniffers are a type of malware written in JavaScript designed to infiltrate and steal card-not-present (CNP) data from the checkout pages of e-commerce websites.



- Perform regular website audits to identify suspicious scripts or network behavior
- Prevent non-essential, externally loaded scripts from loading on checkout pages
- Evaluate third-party plugins on your e-commerce website and monitor for changes in their code or behavior

Automated Marketplaces and Logs Vendors

Online shops and marketplaces are used to buy and sell credentials for bank accounts, cell phone accounts, online store accounts, dating accounts, and even digital fingerprints of compromised systems to facilitate further breaches.

- Monitor shops and marketplaces for accounts relevant to your enterprise
- Act on spikes in the number of accounts available in shops
- Pay attention to credentials for non-public facing domains
- Enable MFA via SMS or authenticator applications

The context provided by threat intelligence helps across all security functions; specifically in the case of incident response, it allows IR teams to evaluate alerts more quickly and confidently. With a threat intelligence solution that automatically gathers and processes data from across the internet, this much-needed context is available in seconds instead of hours or days.

Recorded Future®

recordedfuture.com

@RecordedFuture

About Recorded Future

Recorded Future arms security teams with the only complete security intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.

Background

Since the Industrial Revolution, it has been the aim of businesses to streamline processes to lower costs and increase productivity and profits. Ethics aside, criminal activities are, at their heart, businesses like any other. It is then no surprise that automation has also been part of the cybercriminal underground since its inception, and threat actors have continued to implement new techniques and methods of automation that frequently outpace the efforts to defeat them. Malware that might have once taken weeks or months to develop, test, and implement is now frequently and readily available right off the shelf. As a result, malicious campaigns can be planned and executed more quickly and by less sophisticated threat actors.

Threat actors may no longer need to "hack" a company to get their initial foothold. They can simply buy access to the company from a vendor selling breached access or leaked databases belonging to the target. Instead of spending long hours parsing through these databases manually, they can access criminal shops that have parsed compromised credentials for them, where they can buy not only credentials, but also "digital fingerprints" of the very machines those credentials were stolen from. Then, instead of spending time validating the credentials, they can simply rent a checker against a target company to do so in seconds.

Threat actors can rent loaders and crypters to help deliver and obfuscate their malware. They can choose from a variety of injects or overlays to infiltrate websites and collect vital login or financial information. Or, they can rent ready-made exploit kits prepackaged with the exploits they need to drop the stealer of their choice onto compromised devices and proceed to collect the necessary information that way.

To keep their criminal enterprise running smoothly, threat actors can choose from a myriad of services providing bulletproof hosting and proxy services. To monetize the information they've collected, instead of looking for drops and money mules, they can deliver the information to numerous shops and automated marketplaces where the cycle can begin again.

In other words, the process of executing a cybercriminal campaign has been simplified, automated, and democratized by the proliferation of very specialized services catering to every aspect of the underground economy. In November 2017, Recorded Future analysis demonstrated this specialization, as well as the cost of executing a campaign.

In turn, to more effectively combat these commoditized campaigns, defenders need to arm themselves with the most up-to-date information. Entities need to be able to have timely access to breached data to check for potential compromised accounts belonging to employees. They need to know whether a new checker or inject has come on the market targeting their company. They need to know what new exploits are part of the exploit kits being offered on underground forums — and they need to be able to do all this as quickly as possible.

Threat Analysis

Databases and Network Access

Many cyberattacks ultimately start with a compromised network or a database of credentials obtained from the compromised network offered for sale or auction on dark web forums. In some instances, the databases are released for free on platforms like Pastebin and others. While a database breach is not an attack on its own, but rather the result of threat actors obtaining unauthorized access to a network, the access provides threat actors with the raw material for vectors such as privilege escalation and data exfiltration. Moreover, ransomware operators can use the access to encrypt the compromised network. Hackers can exfiltrate databases with personally identifiable information (PII), personal health information (PHI), corporate documents, email addresses, employee information, social media profiles, as well as usernames and passwords of other services a given organization uses. Usually, all of these malicious incidents are grouped under the category of database breaches or leaks.

Statistics indicate that the number of database breaches increases every year. According to Norton, there were 3,800 publicly disclosed breaches in 2019 with 4.1 billion records exposed. Database breaches are sold or shared among threat actors across the dark web, who can use the username and password combinations typically found in these databases for credential stuffing attacks against popular online services and sites.

Database Sales

Cybercriminals often do not advertise the breaches immediately, instead processing the data internally to extract maximum value first before selling, usually several months later. In many cases, the contents of breached databases are not sold entirely, but rather in sections, such as email accounts with passwords, other PII, or payment card data. Many publicly leaked databases are shared on forums on the dark web.

Notable Threat Actors Selling and Sharing Databases

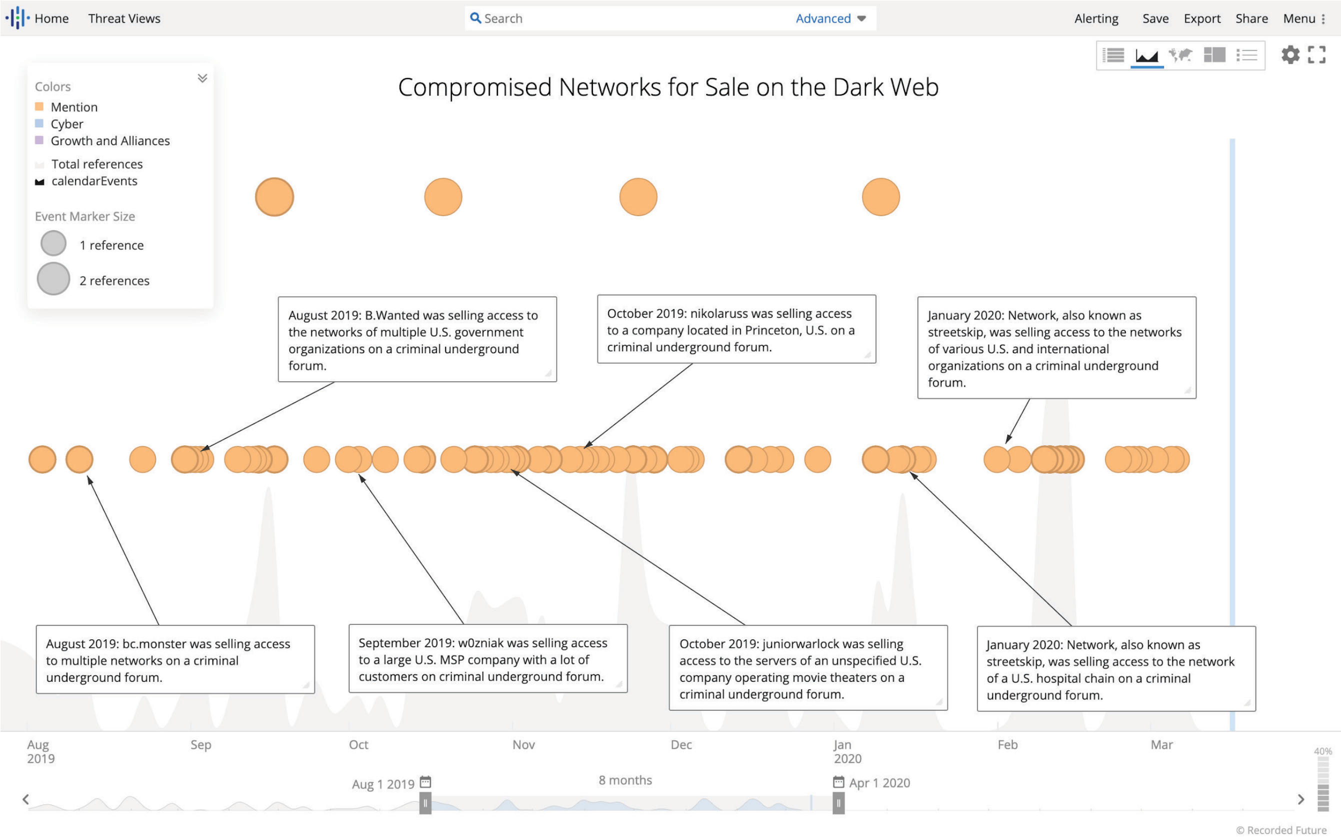
- **Xrenovi4**, a member of several Russian- and English-language forums, has operated cit0day[.]in since 2017, which is an online store dedicated to the sale of leaked email databases.
- **teamkelvinsecteam**, also known as **KelvinSecTeam**, operates a subscription-based service for sales of the hacking tools, malware, and leaked databases from their website kelvinsecurity[.]com, where they offer a wide range of leaked databases primarily related to e-commerce, telecommunications, and other businesses, as well as compromised dark web forums.
- **Omnipotent** maintains an official collection of over 300 databases, each of which forum members can access for a small fee.

Compromised Networks

The sale of access to compromised networks of government, business, educational, and other entities can be a lucrative business on the dark web, where prices vary from a few hundred to hundreds of thousands of U.S. dollars. In these instances, cybercriminals have obtained access to an organization’s network using different methods such as compromised third-party software (such as Citrix, TaxSlayer, or LexisNexis), RDP access, compromised internet routers, or phishing.

Frequently, access to networks is sold on the dark web in the form of an auction where forum members bid against one another, or simply via a direct sale with a set price. Some forums are well known as sources for high-value networks from organizations such as healthcare, insurance companies, law firms, manufacturing, aviation (airlines and airports), education (universities and colleges), government (state and city administrations, police departments, regional healthcare authorities, election committees), e-commerce, and finance (accounting companies and banks).

Notable Sellers



August 2019: B.Wanted was selling access to the networks of multiple U.S. government organizations on a criminal underground forum.

October 2019: nikolaruss was selling access to a company located in Princeton, U.S. on a criminal underground forum.

January 2020: Network, also known as streetskip, was selling access to the networks of various U.S. and international organizations on a criminal underground forum.

August 2019: bc.monster was selling access to multiple networks on a criminal underground forum.

September 2019: w0zniak was selling access to a large U.S. MSP company with a lot of customers on criminal underground forum.

October 2019: juniorwarlock was selling access to the servers of an unspecified U.S. company operating movie theaters on a criminal underground forum.

January 2020: Network, also known as streetskip, was selling access to the network of a U.S. hospital chain on a criminal underground forum.

Top sellers of the compromised networks on the dark web for the last six months. (Source: Recorded Future)

- **“streetskip,”** also known as **“network,”** sells access to the networks of multiple U.S. and international companies.
- **“bc.monster”** sells access to the networks of various U.S. and international organizations, as well as PII and stolen documents.
- **“B.Wanted”** primarily sells access to the networks of U.S. government organizations and law enforcement agencies.
- **“Lalartu,”** a member of various Russian-language forums, sells access to the networks of law enforcement agencies and law firms, and is a participant in ransomware affiliate programs.
- **“ellisdouglas”** sells admin access to the networks of two U.S. and international government entities, and various Russian, Ukrainian, Brazilian, and German organizations.

Mitigation Techniques

Insikt Group recommends the following measures be taken to protect against the exploitation of vulnerabilities targeting organizations' websites and networks resulting in database breaches:

- Keep all software and applications up to date; in particular, operating systems, antivirus software, applications, and core system utilities.
- Filter email correspondence for SPAM and scrutinize links and attachments prior to accessing them; ensure malicious attachment monitoring, if available, is on.
- Make regular backups of your system and store the backups offline, preferably offsite so that data cannot be accessed via the network.
- Adhere to strict compartmentalization of company-sensitive data. In particular, look at what data anyone with access to an employee account or device would have access to (e.g., through device or account takeover via phishing). Verify access control for users, and ensure employees have a business need to access resources.
- Strongly consider instituting role-based access, limiting company-wide data access, and restricting access to sensitive data.
- Monitor vendors' security or assess risks that could be passed on by use of a third-party technology.
- Apply data encryption standards for stored databases to protect it from being used with malicious purposes by individuals who were able to get unauthorized access to the internal network of the organization.
- Monitor available databases for employee accounts.

Business Email Compromise (BEC)

Another TTP closely related to and often facilitated by database breaches and access to networks is business email compromise (BEC). This method often employs social engineering and phishing and attempts to compromise companies by pretending to be a legitimate employee or manager of the company through compromised email accounts. The end goal of this attack is to steal confidential corporate information or initiate money transfers to accounts controlled by cybercriminals.

According to the FBI's Internet Crime Complaint Center (IC3), as of February 27, 2017, "the BEC scam continues to grow, evolve, and target businesses of all sizes," and, "Since January 2015, there has been a 1,300% increase in identified exposed losses, now totaling over $3 billion."

Mitigation Strategies

According to the FBI, these steps will reduce the risk of being compromised by BEC attack:

- Create intrusion detection system rules that flag emails with extensions that are similar to company email.
- Create an email rule to flag email communications where the "reply" email address is different from the "from" email address shown.
- Differentiate the email using color coding and prepended tags in the subject that will help to identify emails from employee/internal accounts and emails from non-employee or external accounts.
- Enable multi-factor authentication (MFA) via SMS or authenticator applications such as Google Authenticator, Duo Mobile, FreeOTP, Authy, or Microsoft Authenticator to securely access devices.
- Confirm requests for transfers of funds by using phone verification as part of a multi-factor authentication; verify the number from other sources, such as the company's website or previous billing or correspondence, not the numbers provided in the email request.

Insikt Group recommends paying particular attention to the following unusual email requests to prevent BEC fraud:

- Requests that bypass normal channels of communication and request immediate actions such as money transfers or the access to documents or information
- Senior level management sending unusual requests, especially to employees who are not their direct reports
- Language, grammar, or format issues revealing errors, typos, and format flaws in emails
- Requests that the recipient not communicate the content of the email to others

Checkers/Brute-Forcers

Overview

Equipped with credentials obtained from data breaches, attackers can now use checkers and brute-forcers directing large-scale automated login requests against websites to determine the validity of victim accounts and gain unauthorized access to them. This type of attack is also known as a credential stuffing attack. According to the Recorded Future report "The Economy of Credential Stuffing Attacks," with an investment of $550, criminals could earn at least 20 times the profit on the sale of compromised login credentials. Akamai reported that it detected over 3.5 billion credential stuffing requests aimed at financial institutions in the past 18 months.

Checkers are automated tools (scripts or software) used by cybercriminals to check the validity of user ID and password combinations against a website's login system. Checkers may use the website's main page, mobile app, or an application program interface (API) function to identify valid accounts.

Brute-forcers are automated password cracking tools that can also be used to discover hidden pages and content in a web application. Cybercriminals use brute-forcers to gain access to confidential information and user accounts through automated server requests. Brute-forcers attempt to guess and crack passwords or usernames using a trial and error method. Automated brute-forcers, such as Brutus, Medusa, THC Hydra, Ncrack, John the Ripper, and Rainbow, help attackers expedite guessing a password for a particular user or site. Partial information such as username obtained from a data dump also makes it easier for an attacker to use a brute-forcer to get the password.

Checkers and brute-forcers allow cybercriminals to automate the reconnaissance phase of an attack and gain additional user details (such as available addresses, emails, and payment card details) or access to the targeted account. In the Cyber Kill Chain Model, reconnaissance is the first step used by cyberattackers to collect information on their intended targets.

Threat actors use automated checkers and brute-forcers available on the criminal underground with the goal of validating accounts and gaining access to them. These types of attacks are possible if victims reuse the same login information across multiple online platforms. According to the University of Southern California research, "password reuse is rampant and indiscriminate; 98% of users reuse their passwords verbatim and 84% reuse an important password at a non-important, and likely less secure site; main causes for password reuse are a poor understanding of risk and preference for memorability over security."

In a credential stuffing attack, a criminal will be in possession of a database of credentials and PII, frequently obtained from a data breach. For example, an attacker could have obtained PII data from the LinkedIn data breach of 170 million credentials compromised in 2012 and leaked on the dark web in 2016 (there were 1,135,936 LinkedIn members using the password "123456"). Then, an attacker can use these credentials to gain access to unrelated accounts such as an email or a bank account. Account checkers and brute-forcers commoditize credential stuffing attacks, aiding with automation for easier and faster ways of gaining access to user accounts and PII. According to Security Intelligence, account checkers may outnumber legitimate login attempts by a factor of greater than four to one.

Recorded Future continuously collects data dumps posted to the dark web, or obtained through special collections sources cultivated by the Insikt Group. These dumps typically contain breached accounts' email addresses and passwords either hashed or in plain text. Recorded Future clients can use these leaked credential dumps to identify how many of their employees' and clients' usernames and passwords have been exposed. Organizations can query their brand names to identify credential leaks, and if identified, prompt the account holder to change their password.

Notable Recent Incidents

On January 30, 2020, TechCrunch reported about a breach at Indian airline SpiceJet that affected 1.2 million passengers. Reportedly, the access to SpiceJet's internal systems was gained by brute-forcing the system's easily guessable password.

In January 2020, Amazon-owned smart camera maker Ring faced a lawsuit from a family whose camera in the children's bedroom was hacked. Allegedly, criminals used a list of common passwords to brute-force their way into the family's Ring camera account.

In July 2019, U.S. banking and insurance company State Farm said it suffered a credential stuffing attack during which "a bad actor" was able to confirm valid usernames and passwords for State Farm online accounts.

Notable Checkers and Brute-Forcers

Cybercriminals will use lists of hundreds and thousands of credentials with automated, custom, and "off-the-shelf" tools available on the dark web. Tools such as STORM, Black Bullet Account Cracker, and Sentry MBA support an unlimited number of custom plugins, known as "configs," which essentially offer cybercriminals the capability to target almost any company with an online retail presence and conduct account takeovers. Additional tools sold on the criminal underground include All-in-One Checker, Starjieu Mail Checker, Private Keeper, SNIPR, WOXY email checker, Slayer Leecher, and Kerbrute. There are also lesser-known tools built to target single companies (like Netflix, Facebook, Instagram, or Spotify).

These automated tools help attackers use compromised usernames and passwords against a range of accounts, including banking, e-commerce, loyalty or rewards programs, social media, and cryptocurrency wallets. Once the attackers obtain access to an account, they try to drain available funds, rewards points, steal personal and financial details (such as credit card data), or commit fraud or identity theft. For automated brute-forcing tools, attackers will often use a list of common passwords with the most common combinations first.

According to the underground forum chatter, it only takes All-in-One Checker 90 seconds to check a database of 5,400 email addresses and return results informing the attacker which accounts are valid and which can be accessed with a brute-forced password. The price for the All-in-One Checker is only $12. It is sold by the seller and developer AN9ROS.

Notable Sellers of Checkers and Brute-Forcers

Insikt Group observed and analyzed the activity of threat actors specializing in the sales of checkers and brute-forcers on the underground forums. Many forums have thousands of threads dedicated to credential stuffing attacks and sales of the corresponding software.

Insikt Group identified and analyzed the activities of three prominent cybercriminals, among multiple threat actors specializing in credential stuffing attacks and sales of checkers and brute-forcers on the underground forums:

- **“bruteguru”** is the vendor of a brute-forcer and account checker tool known as “Guru Brute B&C.” This tool targets popular CMS panels such as Magento, WordPress, Drupal, Joomla, OpenCart, Bitrix24, cPanel, WHM, and WooCommerce, along with other services such as FTP, SSH, and MySQL.
- **“SaNX”** sells API exploits that can be used for brute-forcing accounts with the generation of the necessary tokens that mimics a login of an official program. The actor has been observed offering “private API” for approximately 30 companies.
- **“getsend”** is offering services in developing checkers and brute-forcers.

Mitigation Strategies

- Increase awareness among the users and clients to use unique passwords for each of their accounts. A password manager would help end users generate, store, and retrieve unique and complex passwords.

- Use Recorded Future to surface compromised credentials from database breaches, and once identified, take appropriate action to address the threat.
- Require additional details (for example, CAPTCHA or the user's last name) during the login process to break the attacker's programmed logic in automated credential stuffing attacks.
- Use multi-factor authentication if possible.
- Establish customized web application firewall rules, with special attention to unusual header orders and user-agents, as well as checking for valid referrers.
- Intentionally slow down or rate limit login traffic to discourage attackers. For example, lock out accounts after a certain number of failed login attempts or introduce a delay in server responses to login requests.
- Remove unused public-facing login paths and tighten controls on the mobile and API login paths.
- Baseline traffic and network requests in order to monitor the web service for unexpected traffic, including volume and request type.
- Use Recorded Future to monitor criminal underground communities for the availability of new configuration files targeting your organization, acquisition, and the thorough analysis of such files for additional attack indicators.

Loaders and Crypters

Once threat actors have identified a target, their next step is frequently delivering the malicious payload, such as malware, to the target system or device. Since many of the targeted systems or devices are protected to some extent by antivirus software, which may recognize, flag, or block the malicious payload, threat actors typically apply special tools such as loaders and crypters as part of the initial infection to elude detection by endpoint security products and then download and execute one or more malicious payloads.

Loaders

Loaders usually contain a limited set of capabilities. They are generally responsible for surveying a victim's computer, checking in with a command and control (C2) server, and then downloading and executing more advanced malware. The exact details of this process vary from loader to loader, but the most basic loaders might save the final payload to the victim's file system and then run it as a new process. The most advanced loaders will keep the downloaded payload entirely in-memory, and execute it using a process injection technique like process hollowing or reflective DLL injection. By keeping the payload in memory, the loader reduces the chances that security products could detect the final payload.

Notable Loaders

- **"Amadey,"** sold by the threat actor **"InCrease,"** is a loader with basic upload, download, and autorun functionality that costs $600.
- **"DiamondFox,"** sold by the threat actor **"edbitss,"** is a multifunctional loader with optional custom modules such as a RAM scraper, ransomware, cryptojacker, and some stealer functionality including browser password and cookie grabbing. DiamondFox costs as low as $600 for the base version, or as high as $2,700 with all add-on modules.
- **"Buer Loader,"** sold by the threat actor **"memeos,"** is a basic loader that is executable as a DLL or EXE file, detects sandbox environments, runs with user privileges, and has the option to choose which countries and operational systems to infect. Buer Loader costs $400, which gives buyers free lifetime technical support, updates, and bug fixes.
- **"Smoke Bot,"** sold by the threat actor **"SmokeLdr,"** is a multifunctional loader with optional custom modules such as a form grabber, password stealer, and DDoS capabilities. Smoke Bot costs as low as $400 for the base version, or as high as $2,450 with all add-on modules.

Crypters and No-Distribute Scanners

Crypters and no-distribute scanners are two essential services for threat actors involved in propagating malware. Crypting services are used to encrypt and obfuscate malware payloads to avoid detection by antivirus software. Some functionalities of crypters include: to compress executables to reduce size of deliverable, to evade sandboxing through virtual machine detection, and to masquerade as normal software. No-distribute scanners can then be used to check if the crypted malware is being detected by any antivirus software, and is discussed in detail in the Insikt Group report "Uncover Unseen Malware Samples With No Distribute Scanners."

As the number of attack surfaces has continued to increase, more threat actors are using innovative attack vectors to deploy new variants of malware. Some of these threat actors do not possess technical expertise and need the expertise of more technical threat actors to deploy malware. Thus, developers of crypters create products designed to be used by threat actors of varying technical sophistication. These crypters are often user friendly and provide a simple interface that includes the GUI that configures all the options, including encryption methods, key, and where to inject the payload. Once a threat actor has selected a crypter and uploaded the necessary information, the following generally happens:

- The crypter encrypts the malicious payload into a functioning programming code
- The threat actor delivers this program to victims via phishing or spamming
- The crypter decrypts itself and releases the malicious payload once executed

Notable Crypter and No-Distribute Services

- **"Kerens"** operates the no-distribute service avcheck[.]net and the crypter service crypt[.]guru.
- **"p1t"** operates the crypter service KleenScan, located at kleenscan[.]com.
- **"dyncheck"** operates the no-distribute service "Dynamic Runtime Antivirus Check," located at dyncheck[.]com.

Mitigation Strategies

- Update antivirus software regularly, given the large number of customized crypters (as well as tutorials and how-to guides) readily available to the public via open sources and developers of crypters continuing to produce crypters with enhanced features to defeat antivirus measures.
- Although crypters are designed to defeat antivirus scanning, other incident response and detection controls may be able to detect the unpacked payload at runtime, like a network intrusion detection system (IDS), endpoint monitoring, netflow collection, host logging, and web proxy, alongside human monitoring of detection sources.
- Train and educate individuals on the risks associated with phishing, as this is the initial access point in which malware encrypted by crypters is deployed.

Stealers

Stealers are another popular tool among cybercriminals used to exfiltrate sensitive information from victims, as well as a method for installing secondary payloads onto victim systems. These pieces of malware are often preconfigured to steal a wide variety of login credentials from popular online services, email clients, and file management software, along with other valuable assets such as cryptocurrency wallets. Stealer creators typically provide software updates and customer support continuously to ensure the malware is functioning properly. This type of malware essentially acts like a remote access trojan in that it gives the attacker the ability to remotely interact and control a compromised computer or cellular device.

Notable Stealers

- Raccoon Stealer, sold by the threat actor group "**raccoonstealer**," is one of the more popular stealers on the dark web, and can steal emails, passwords, credit card data, and cryptocurrency wallets, as well as system information. The stealer is widely advertised in Russian-language forums and is believed to be controlled by Russian-speaking threat actors.

- KPOT, known for stealing data from web browsers, instant messengers, email, cryptocurrency, and the VPN on a victim's host. Its functionality has been developed and sold by the threat actor "**MonsterCat**," and is a configurable remote access trojan capable of stealing credentials from a wide variety of system applications including VPN, email, RDP, cryptocurrency wallets, FTP, and social media applications.
- Predator the Thief, created by the threat actor "**Alexuiop1337**," steals cookies, usernames, and passwords from Edge, Chromium-based browsers, and Gecko-based browsers. Predator can steal login credentials from FTP clients, chat applications, VPN clients, or cryptocurrency wallets, and also collects victim system information.
- AZORult is an information stealer that can steal credentials from several software applications, enumerate and steal files from the desktop, capture saved data from browsers (including cookies, passwords, and saved credit card information), steal Skype login credentials, and steal cryptocurrency wallet information.

Mitigation Strategies

Mitigation strategies against stealer malware include the following:

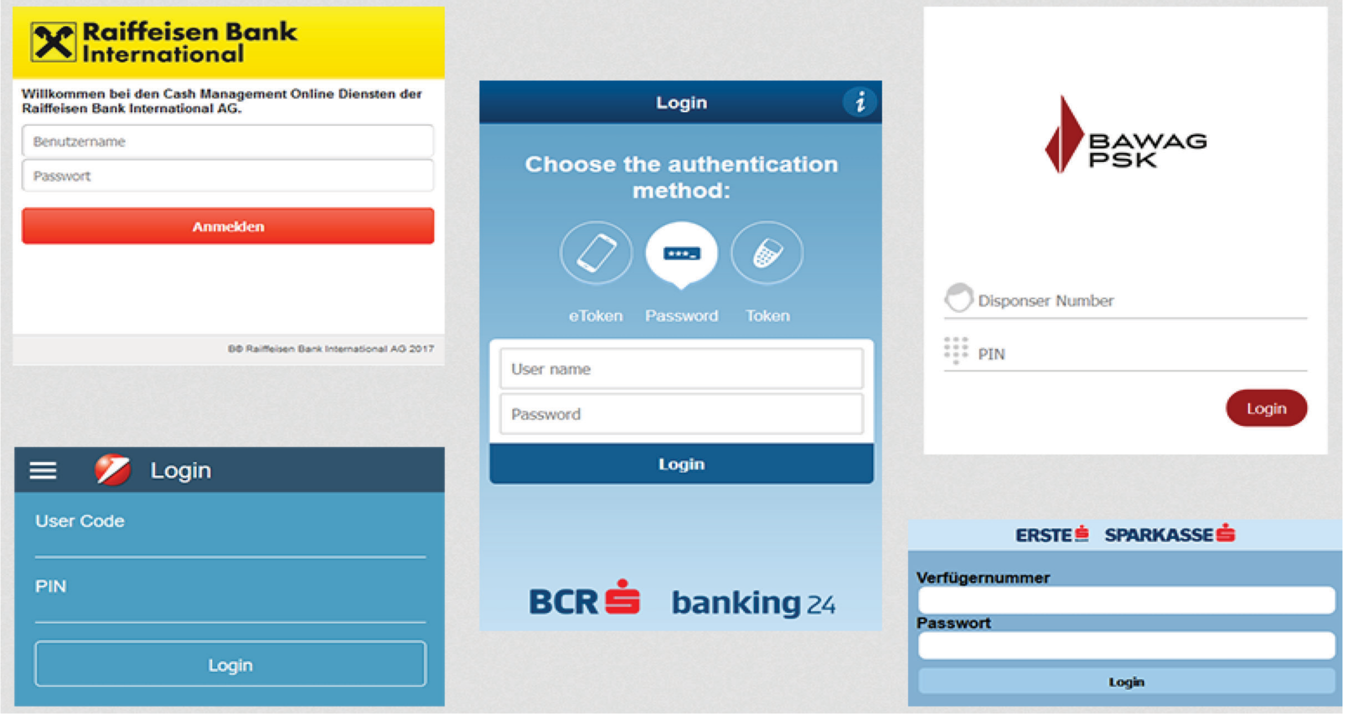
- Invest in a solution that offers patch posture reporting. This type of solution can provide insight into the vulnerabilities that have received remediation measures as well as the machines that have received those patches.
- Configure intrusion detection systems (IDS), intrusion prevention systems (IPS), or any network defense mechanisms in place to alert on any malicious activity.
- Monitor for suspicious changes to system file drives and Registry that focus on the interception of keystrokes.
- Use Recorded Future for the detection of compromised credential information linked to valid accounts and to assist in providing context surrounding suspicious user behavior that may include keylogging activity. Recorded Future platform users can continue to monitor underground sources to identify the spyware and keylogging tools that are likely to have the greatest impact to their immediate infrastructure or supply chain.

Banking Injects

Banking injects are popular and powerful tools for performing fraud and are widely available on the dark web. Banking injects are modules that are typically used with banking trojans for the injection of HTML or JavaScript code into content before it is redirected to a legitimate bank website. Typically, a web inject would serve as an overlay, resembling a legitimate bank login page and requesting input of additional confidential data such as payment card data, Social Security numbers (SSN), PINs, credit card verification codes (CVV), or any other PII, even if it is not required by the bank.

Banking injects are part of a man-in-the-browser (MitB) attack in which the banking trojan can modify the content of the legitimate bank page in real time by performing API hooking. Modified infected content that is going to be added to the legitimate page is located in a web inject configuration file, which is typically hosted on a remote command and control (C2) server and downloaded to the infected machine or device. The attackers can update the configuration files on the server and on the infected machines automatically. Cybercriminals encrypt and obfuscate configuration files in order to evade detection by antivirus software and make analysis more difficult.

Analysis indicates that banking web injects are currently integrated with multiple banking trojans, allowing both the compromise of the user's bank account and the use of Automatic Transfer Systems (ATS) to steal money automatically. Among the most popular banking trojans usually integrated with web injects are Cerberus, Anubis, Mazar, ExoBot, and Loki Bot. Some web injects can successfully bypass two-factor authentication (2FA). Web injects that are integrated with banking trojans have control panels and can obtain full control over the user machine. Analysis of the dark web market indicates that some banking inject developers on the criminal underground offer both off-the-shelf injects as well as customized injects created individually for each customer. These products are significantly more expensive, and prices can reach up to $1,000, whereas the average price for these types of web injects is $150-250.



Willkommen bei den Cash Management Online Diensten der Raiffeisen Bank International AG.

Austrian bank inject pack created by the actor Validolik.

Notable Threat Actors

- "**Validolik**": A member of several top-tier Russian-language forums, this threat actor is one of the leading developers of Android web injects.
- "**Pw0ned**": A Russian speaker and moderator on a criminal underground forum. The threat actor is primarily known as a developer of bank web injects and fake pages of popular social media such as Instagram and VKontakte (VK), and email service providers such as Gmail, AOL, and Yandex.
- "**Kaktys1010**": The threat actor is a member of several top-tier Russian-language forums and is the developer of Windows and Android web injects, as well as fake pages with and without SMS/token interception. The actor operates the onion website KTS (o54eavgyktxh5wts[.]onion/shop) for sales of the above-mentioned products.

Mitigation Strategies

- Keep all software and applications up to date; in particular, operating systems, antivirus software, applications, and core system utilities.
- Install an antivirus solution, schedule signature updates, and monitor the antivirus status on all equipment.
- Enable MFA via SMS or authenticator applications such as Google Authenticator, Duo Mobile, FreeOTP, Authy, or Microsoft Authenticator to securely access devices.
- Use only an HTTPS connection on the internet.
- Educate employees and conduct training sessions with mock phishing scenarios.
- Deploy a spam filter that detects viruses, blank senders, and so on.
- Deploy a web filter to block malicious websites.
- Encrypt all sensitive company information.
- Convert HTML email into text-only email messages or disable HTML email messages.
- Require encryption for employees.
- Only download apps and files from trusted sources.
- Use a password manager. Most banking trojans can log keystrokes; by using a password manager to fill in passwords, you avoid physically typing in credentials, which essentially renders a keylogger useless.
- Compare the bank’s login screen on your computer with the same login screen on someone else’s to ensure they look the same.

Exploit Kits

Exploit kits (EKs) are toolkits that automate the exploitation of web browser vulnerabilities to maximize successful infections. These toolkits serve as a platform to deliver malicious payloads such as trojans, loaders, ransomware, and other malicious software, frequently done so via malvertising, compromised websites, or malicious URLs in spam. Common exploit kits observed by Insikt Group in the last few years include FalloutEK and RIG EK.

Threat Actors Advertising the Sales of Exploit Kits

Recorded Future's Insikt Group identified two threat actors that have been historically observed developing and selling exploit kits on underground forums:

- **"FalloutEK"**: Recorded Future data indicates that the threat actor FalloutEK is the creator and operator of the Fallout Exploit Kit (FEK), which is sold exclusively on the Russian-language Exploit[.]in. Fallout Exploit Kit has received positive community feedback, with a user base that includes the ransomware-as-a-service (RaaS) affiliate programs GandCrab and Kraken Cryptor. FalloutEK is known to work with partners that advertise the sales of the FEK, such as A. Server and GandGrab, both of whom have touted their successful usage of the FEK.
- **"TakeThat"**: In December 2019, the threat actor TakeThat was observed by Recorded Future advertising the sales of a newly released version of the RIG Exploit Kit, dubbed RIG Exploit Kit v.4.0 on some forums. In these advertisements, the actor stated that the new version of the exploit kit has enhanced capabilities, such as the ability to target all Windows versions (32/64-bit), bypass User Account Control (UAC), and has an API functionality and automated link generation. TakeThat claimed that the average successful infection rate was approximately 10% to 15%.

Trend Analysis: The Decline of New Exploit Kits

Even though analysts have observed exploit kits available for rent, such as TakeThat advertising the rental of the RIG Exploit Kit for a little as $100 per day, $400 per week, and $1,200 per month, Insikt Group has seen a decline in the creation of new exploit kits. Furthermore, in the last few years, Recorded Future analysts identified a shift in preference among cybercriminals from these exploit kits targeting Adobe vulnerabilities to Microsoft consumer product exploits. In 2017, analysts first observed that these criminal exploit kits and phishing campaigns favored Microsoft products, with seven of the top 10 vulnerabilities exploited by phishing attacks and exploit kits using Microsoft products, as seen in our rankings. This is in stark contrast to our previous rankings (2015, 2016), which saw consistent exploitation of Adobe Flash vulnerabilities. Analysis of these sources from January 1, 2017 to December 31, 2017 identified Adobe as a still popular but declining avenue of attack, with the remaining three vulnerabilities tied to the aging Flash Player.

In 2018, the number of new exploit kits continued to drop by approximately 50%, with only five new exploit kits released, compared to 10 the year before. Two of these exploit kits were associated with 2018's top exploited vulnerabilities: Fallout and LCG Kit. As in previous years, similar trends continue to impact the downward trend of exploit kits, including shifts to more secure browsers and specific victim targeting. Even so, analysts identified that, within these exploit kits, Microsoft vulnerabilities continued to be the most exploited, per Recorded Future research. The top exploited vulnerability in 2018 was CVE-2018-8174, a Microsoft Internet Explorer vulnerability nicknamed "Double Kill," which was included in four exploit kits (RIG, Fallout, KaiXin, and Magnitude). Unlike our observations in 2017, analysts only observed one vulnerability tied to Adobe Flash on this year's list. Tracked as CVE-2018-8174, this vulnerability was included in multiple exploit kits, most notably the Fallout exploit kit, which was used to distribute GandCrab ransomware.

Mitigation Strategies

- Given the trend observed by Insikt Group analysts of Microsoft exploits appearing in our Top 10 Exploits reports for the past three years, prioritize the patching of Microsoft products in your technology stack.
- Ensure that Adobe Flash Player is automatically disabled in your browser settings. Additionally, as Adobe will end support for Flash Player on December 31, 2020, it is not recommended to download or continue to use this product.
- Do not forget to patch older vulnerabilities — the average vulnerability stays alive for nearly seven years, according to a 2017 RAND report.
- Conduct or maintain phishing security awareness to mitigate attacks. This can include user training to encourage skepticism of emails requesting additional information or prompting clicks on any links or attachments. Companies will not generally ask customers for personal or financial data, but when in doubt, contact the company directly by phone and confirm if they actually need the information.
- Vulnerability management teams can use Recorded Future's technical intelligence to prioritize patching based on which vulnerabilities are actively being exploited in the wild by malware.

Spam and Phishing

Spamming and phishing (including spearphishing) are often coupled together, but in reality, they are very different tools.

Spam

Threat actors who typically participate in spamming will usually target thousands of victims at the same time indiscriminately. Spam content typically involves online pharmacies, pornography, dating, gambling, "get rich quick" schemes that involving working from home, chain emails, hoax viruses, and more.

Spammers are often able to obtain email information through the following methods:

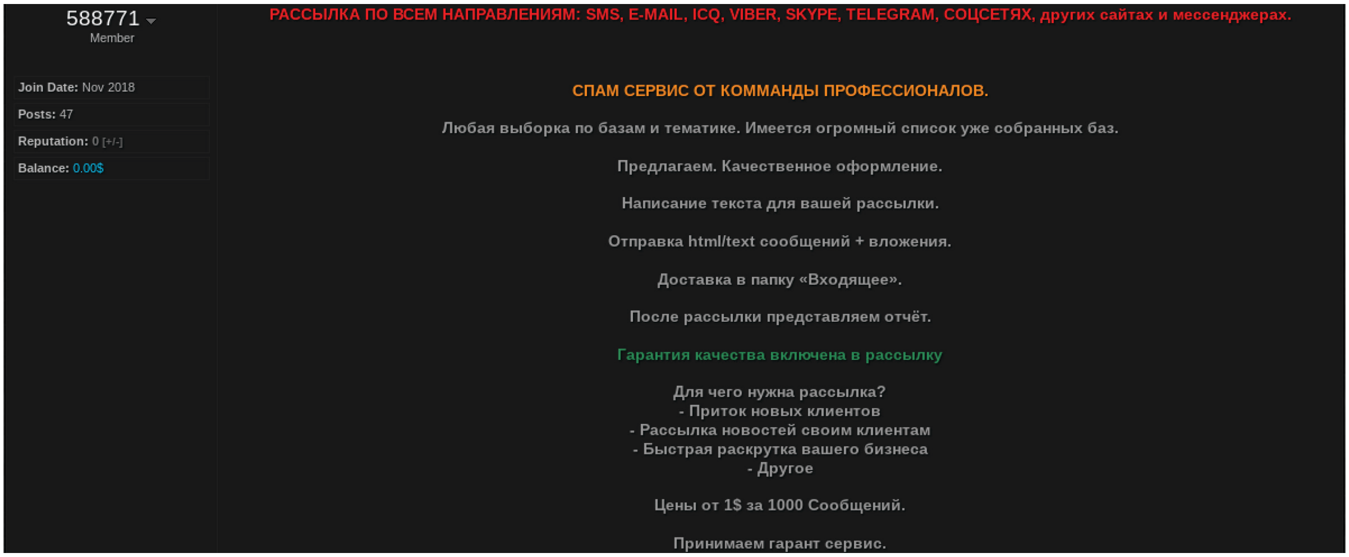
- Using automated software to generate addresses
- Enticing people to enter their details on fraudulent websites
- Hacking into legitimate websites to gather users' details
- Buying email lists from other spammers
- Inviting people to click through to fraudulent websites posing as spam email cancellation services
- From names/addresses in the cc line, or in the body of emails which have been forwarded and the previous participants have not been deleted

The very act of replying to a spam email confirms to spammers that your email address exists. This method can be used to validate the legitimacy of a data breach or data dump in which account credentials are at least partially available.

Recorded Future analysts identified Xrumer and FlowerPippi as examples of commonly used spamming malware tools used to target unsuspecting internet users.

Threat actors engaging in spam activities:

- **"588771"** is a Russian-speaking cybercriminal who specializes in professional spam services targeting SMS, email, Skype, Telegram, and social networks, in addition to other sites and other prominent instant messengers. This individual's spam service includes already assembled databases to promote spam for fast business promotion. Prices for 588771's services originally began at $1 for 1,000 SMS messages but are now advertised at $1,000 for 10,000 SMS messages, available in both English and Russian.
- **"stone"** is a Russian-speaking cybercriminal observed selling email spam bots for $2,000. stone claims these bots can randomize the subject, the text of the email, and the name of the attachment. Users of these spam bots can also customize the email's X-Mailer line in the header of an email, specify the number of email threads for one bot, and "much more."



588771
Member

Join Date: Nov 2018
Posts: 47
Reputation: 0 [+/-]
Balance: 0.00$

РАССЫЛКА ПО ВСЕМ НАПРАВЛЕНИЯМ: SMS, E-MAIL, ICQ, VIBER, SKYPE, TELEGRAM, СОЦСЕТЯХ, других сайтах и мессенджерах.

СПАМ СЕРВИС ОТ КОММАНДЫ ПРОФЕССИОНАЛОВ.

Любая выборка по базам и тематике. Имеется огромный список уже собранных баз.

Предлагаем. Качественное оформление.

Написание текста для вашей рассылки.

Отправка html/text сообщений + вложения.

Доставка в папку «Входящее».

После рассылки представляем отчёт.

Гарантия качества включена в рассылку

Для чего нужна рассылка?
- Приток новых клиентов
- Рассылка новостей своим клиентам
- Быстрая раскрутка вашего бизнеса
- Другое

Цены от 1$ за 1000 Сообщений.

Принимаем гарант сервис.

588771's professional spam service advertised on Club2CRD.

Mitigation Strategies

- Refrain from giving out or posting your email address publicly, including on social media.
- Do not reply to spam messages and exercise use of "spam" folders.
- Download additional spam filtering tools and antivirus software to scan incoming emails.
- Avoid using personal or business email addresses when registering in any online contest or service.

Phishing

Phishing is typically conducted similarly to spam, with criminals sending emails to thousands of victims. Phishing attacks frequently use social engineering tactics, emulating emails from trusted or otherwise legitimate entities.

Direct emails to a specific victim, particularly emails to prominent individuals, are referred to as spearphishing. Spearphishing is less likely to originate from automated tools, as these are generally well-crafted, individualized emails tailored to the specific target. Phishing emails appear to be sent from banks, credit card companies, online shops and auction sites, as well as other trusted organizations. They usually try to trick a victim into going to the site, for example to update a password to avoid the account being suspended or to download an important document in an attachment. The embedded link in the email itself goes to a website that looks exactly like the real thing but is actually a fake site designed to trick victims into entering personal information or to download malicious files.

Phishing remains one of the most popular attack vectors for threat actors to conduct social engineering attacks, deploy malware, and gain further access into a target company's network. Ghost Phisher and Gophish are two examples of commonly used phishing frameworks and tools used to target unsuspecting internet users.

The following list includes a few threat actors known to engage in phishing activities:

- **"Poseidon"** is an English-speaking cybercriminal who specializes in creating and selling phishing tools, financial fraud documents and methods, and how-to tutorials and guides on conducting fraudulent activities. Additionally, Poseidon is allegedly capable of carrying out DDoS attacks against websites and is proficient in graphic design, which this actor employs for forging Canadian identification documents and creating phishing pages targeting financial institutions.
- **"frod"** is a Russian-speaking cybercriminal who advertises bulletproof hosting services for phishing operations, in addition to spam, malware, botnets, and spoofing activities for other cybercriminals. Prices for frod's hosting ranges between $75 to $200, depending on buyer requirements.

There are a number of threat actors on numerous markets that advertise and sell phishing pages for certain banks, retailers, and other organizations that have web-based logins. These can be remade and updated to reflect graphic changes to make them the most convincing for potential victims. Threat actors engaging in phishing attacks are not required to do the majority of the legwork. Rather, threat actors with minimal market knowledge can easily identify and pursue services which make targeting easier, faster, and from a business perspective, increases their criminal profit margin.

Mitigation Strategies

- Educate your employees and conduct training sessions with mock phishing scenarios.
- Deploy a spam filter used to detect indicators of phishing, such as viruses, blank senders, and keyword text triggers.
- Keep all systems current with the latest security patches and updates.
- Install an antivirus solution, schedule signature updates, and monitor the antivirus status on all equipment.
- Develop a password security policy that illustrates credential best practices, such as password complexity requirements.
- Deploy a web filter to block malicious websites.
- Require encryption for employees, especially employees working remotely. This includes whole-disk encryption such as 256-bit AES and network encryption via SSL or TLS.
- For enterprises, Recorded Future can monitor for potential typosquat domains weaponized in phishing attacks. This includes not only the domains belonging to one organization, but third-party partners and vendors with enterprise network access.

Bulletproof Hosting Services

To extend the longevity of their criminal enterprises, threat actors have turned to proxy and bulletproof hosting services (BPHS) to help obfuscate their activities and to keep them from being shut down by law enforcement. One of the greatest distinctions between bulletproof hosting service operations and the services offered by a "regular" web hosting provider is the leniency they grant toward the specific data they allow to be hosted on their servers. Previous Recorded Future research has shown that such services often use geo-spoofing techniques to create a wide pool of IPs and are commonly advertised to both entry-level and highly technical underground sources.

Threat actors know that these services are offered in jurisdictions outside the purview of many federal law enforcement agencies, relying on a model that promises not to comply with legal requests that would either disrupt their operations or result in arrests. Some countries offer a middle-ground option as well, requiring administrators of these potential services to establish legitimate businesses within the country in question and only requiring routine check-ins or disclosures of business operations to government officials. Criminal forums, Jabber servers, banking trojans, and other criminal operations all could not exist without hosting, and those individuals who use these services could not use them securely without some sort of network anonymity.

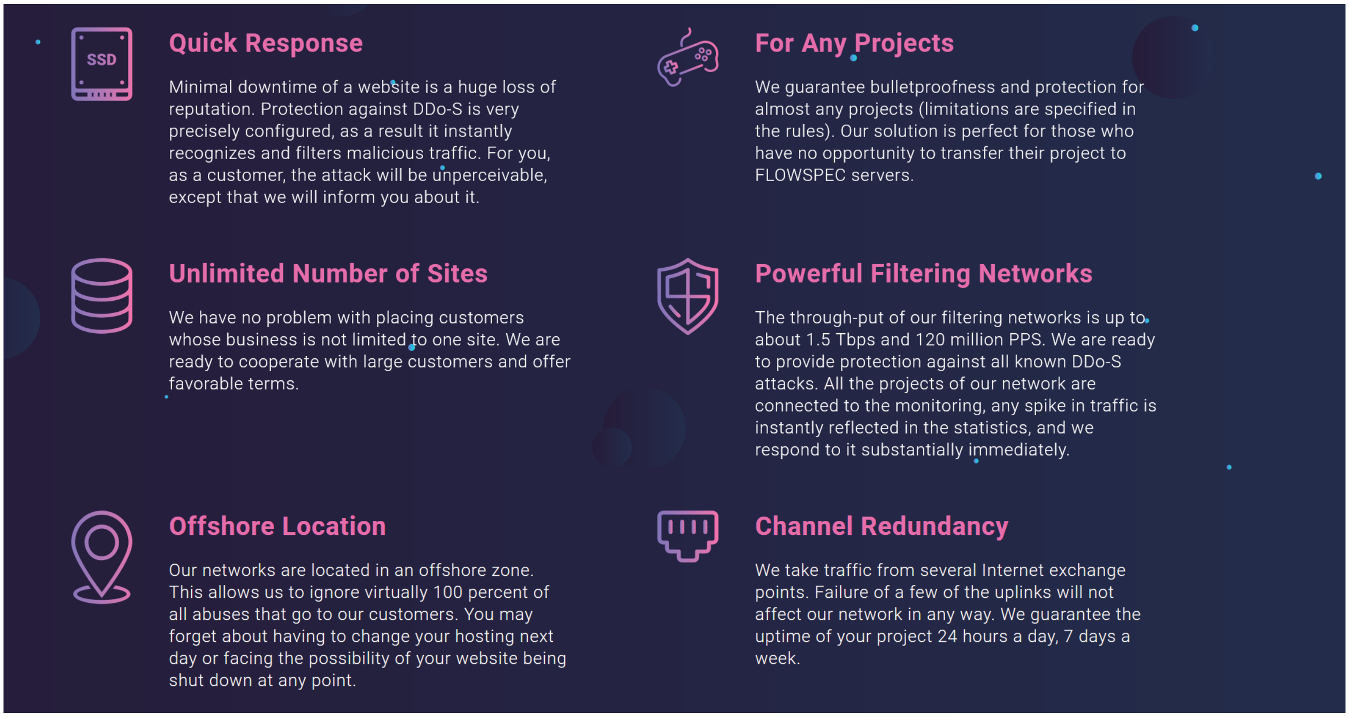
Prominent examples of services enabled via this form of hosting include the following:

- Brute-force attack tools
- Botnet infrastructure
- Exploit kits
- Spamming services

Fast-flux hosting services continue to hinder takedown efforts against nefarious storage services related to malware storage or underground marketplaces, allowing infrastructure like C2 domains to be constantly cycled through an ever-changing series of IP addresses. Members of high-tier Russian-language forums have consistently continued to advertise fast-flux hosting services over VPN configurations, and servers located in every corner of the globe continue to remain a vital commodity within underground communities.

In July 2019, open source reporting indicated an arrest was made of a Ukrainian national accused of orchestrating a prominent underground hosting service responsible for enabling services for 40% of the Russian-speaking “dark web,” demonstrating the vital role that even a single hosting service can play in the support of underground cybercriminal enterprises.

As seen in the visuals below, which are linked to the FLOWSPEC[.]ru hosting service, it has become normal for BPHS to aspire to appear as legitimate as possible, often invoking a strong sense of professional web development to visitors discovering this particular service for the first time. Reputation within the cybercriminal community plays a strong role in determining which BPHS are more likely to thrive over extended periods of time, with recommendations on forums contributing to the overall success of a BPHS on a regular basis.



Quick Response

Minimal downtime of a website is a huge loss of reputation. Protection against DDo-S is very precisely configured, as a result it instantly recognizes and filters malicious traffic. For you, as a customer, the attack will be unperceivable, except that we will inform you about it.

For Any Projects

We guarantee bulletproofness and protection for almost any projects (limitations are specified in the rules). Our solution is perfect for those who have no opportunity to transfer their project to FLOWSPEC servers.

Unlimited Number of Sites

We have no problem with placing customers whose business is not limited to one site. We are ready to cooperate with large customers and offer favorable terms.

Powerful Filtering Networks

The through-put of our filtering networks is up to about 1.5 Tbps and 120 million PPS. We are ready to provide protection against all known DDo-S attacks. All the projects of our network are connected to the monitoring, any spike in traffic is instantly reflected in the statistics, and we respond to it substantially immediately.

Offshore Location

Our networks are located in an offshore zone. This allows us to ignore virtually 100 percent of all abuses that go to our customers. You may forget about having to change your hosting next day or facing the possibility of your website being shut down at any point.

Channel Redundancy

We take traffic from several Internet exchange points. Failure of a few of the uplinks will not affect our network in any way. We guarantee the uptime of your project 24 hours a day, 7 days a week.

FLOWSPEC hosting features.
(Source: flowspec[.]ru)

Within the past six months, Recorded Future has observed a consistent volume of references to actors within underground sources seeking recommendations for a new bulletproof hosting service, though analysts did observe that there was a greater tendency for actors on entry-level English-language forums to seek assistance. It's likely that actors operating within high-tier forums are less likely to openly discuss recommended hosting services they use unless incentivized, given the unnecessary risk or attention it may bring to a useful service in the long term.

Notable Sellers/Services

- **"EliteVPS"**: EliteVPS is a hosting company that has continued to actively advertise its services on underground forums since at least December 2017. Unlike other services, the terms of service associated with their business claim to enforce bans against the dissemination of data pertaining to violence against children and animals.

- **"Yalishanda"**: Yalishanda is an underground actor known to historically advertise hosting services on Exploit and multiple other Russian-language forums since as early as December 2018. Using FastFlux technology, the user has claimed to have their own proxy server that relies on KVM and XEN virtualization. Three domain registrars located in Europe, China, and Malaysia have been affiliated with the actor, representing a variety of geographic diversity in the geographic locations that likely host their malicious infrastructure.

Mitigation Strategies

Underground bulletproof hosting services will often advertise the capability to migrate infrastructure as a key component of their service, enabling interested parties to choose and register their own subnet of IP addresses. Though full mitigation of malicious services hosted within countries more inclined to allow criminal actors to conduct their underground business is virtually impossible without the intervention of regulatory or law enforcement agencies, the Recorded Future Platform can assist in the monitoring of malicious service providers likely disseminating data linked to these businesses (regardless of whether the traffic is unintentional). The crux of this monitoring is often contingent on entire network allocations and the high volumes of malicious services they become affiliated with (such as the ones listed above) becoming unilaterally blacklisted. Recorded Future recognizes that this is not always a viable option, particularly as criminal actors have grown reliant on renting rather than owning this hosting infrastructure.

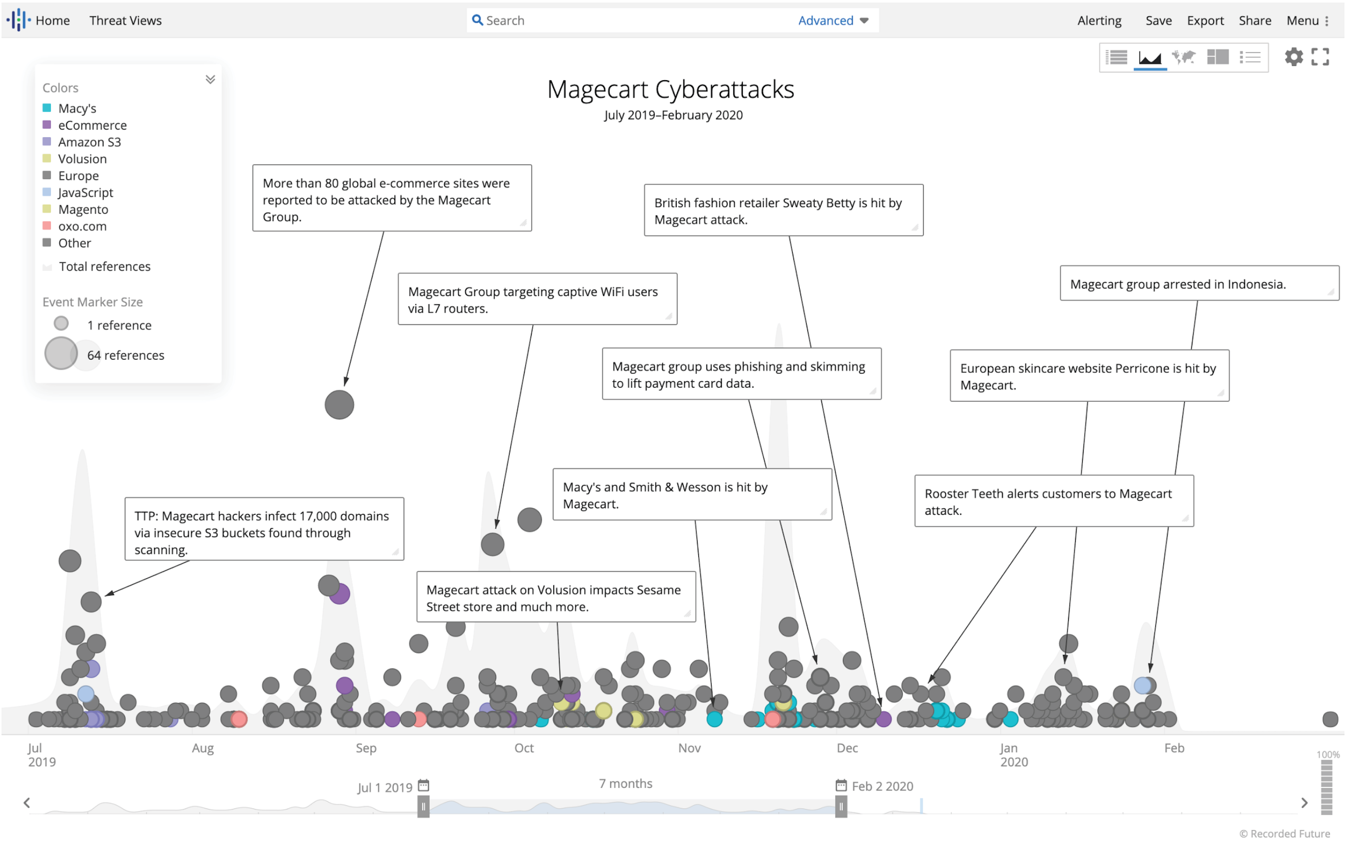
Other takeaway strategies that can reduce the threat posed by bulletproof hosting services and more specifically fast-flux hosting include the following:

- Recorded Future Platform users can mitigate the risk posed by network traffic affiliated with hosting services linked to malicious activity by reviewing Security Control Feeds available through risk rules on Intelligence Cards in addition to the Browser Extension to all users of the Recorded Future Platform. For example, one of Recorded Future's Third-Party Risk Rules is triggered when an IP address belonging to the company has recently been observed communicating to a known malware command and control server on uncommon ports.
- Blacklisting servers affiliated with known-malicious BPHSes continues to be a subject of discussion surrounding the mitigation of these BPHS services. It has become increasingly simple for cybercriminals to migrate infrastructure if detected by security organizations, particularly for those operating multiple servers around the globe simultaneously. If risk rules or alerts within the Recorded Future Platform inform a client or prospect of likely malicious activity affiliated with a hosting service, they are encouraged to contact the appropriate law enforcement entity to assist with takedown operations if necessary.
    - Blacklisting is not limited to server information, with cybercriminals occasionally having the bad habit of signing up for multiple services or subscriptions with the same contact information such as an email address. This information can be monitored within the Recorded Future Platform and assessed with a higher degree of confidence to consistently be linked to the same criminal operation over an extended period of time.

Credit Card Sniffers

In the underground economy, “sniffers” generally refer to a type of malware written in JavaScript designed to steal card-not-present (CNP) data from the checkout pages of e-commerce websites. This CNP data (known as “CVVs”) can then be used to purchase valuable and/or high-demand items online for resale. Once a threat actor has identified a vulnerability that is exploitable by a sniffer, they then inject malicious JavaScript that automatically captures the data from all of the customers who visit the infected site, allowing for the automated collection of the payment card and personal information of numerous customers. The sniffer then forwards the compromised data to the threat actor’s C2 for further exploitation.

Frequently, the different threat actor groups using various types of sniffers have been referred to generically as “Magecart.” Although this attack vector seems prevalent, given that there are at least 12 Magecart-related groups and reported attacks have continued to increase, there are very few threat actors who build, sell, and maintain these sniffers.



More than 80 global e-commerce sites were reported to be attacked by the Magecart Group.

British fashion retailer Sweaty Betty is hit by Magecart attack.

Magecart Group targeting captive WiFi users via L7 routers.

Magecart group arrested in Indonesia.

Magecart group uses phishing and skimming to lift payment card data.

European skincare website Perricone is hit by Magecart.

Macy's and Smith & Wesson is hit by Magecart.

Rooster Teeth alerts customers to Magecart attack.

TTP: Magecart hackers infect 17,000 domains via insecure S3 buckets found through scanning.

Magecart attack on Volusion impacts Sesame Street store and much more.

Notable Magecart activities and attacks from July 2019 to February 2020. (Source: Recorded Future)

Notable Sniffer Developers and Vendors

- **"Sochi"**: Recorded Future data indicates that the threat actor is the creator of the JavaScript sniffer "Inter" and the Android trojan "Red Alert." Some of Inter's attributes are: steals CNP payment data, does not interfere with or drop SSL connections, detects payment forms and card type, and is undetectable by antivirus software.
- **"poter"**: Recorded Future data indicates that the threat actor is a Russian speaker who advertises their "universal sniffer" on Exploit. The sniffer is able to reset activities when the browser is opened, updates when new compromised data retrieved, and searches compromised shops automatically.
- **"Billar"**: Recorded Future data indicates that the threat actor is a Russian speaker who specifically advertises the sniffer variant "mr.SNIFFA," with the threat actor continuing to develop the sniffer to the present day.
- **"Roshen"**: Recorded Future data indicates that the threat actor is a Russian speaker that has been advertising an unnamed but customized sniffer since August 2018 on Exploit. The threat actor includes the following user friendly description of the sniffer's interface: add/delete users, restrict certain users, format export data, and a map view of data.

Mitigation Strategies

Below are mitigation strategies that can assist in preventing a sniffer attack:

- Perform regular audits of your website, including test purchases to identify any suspicious scripts or network behavior.
- Prevent any non-essential, externally loaded scripts from loading on checkout pages.
- Evaluate how third-party plugins use their code, servers, and external communications on your e-commerce website, and monitor for any changes in their code or behavior.

Automated Marketplaces/Logs Vendors

One of the biggest challenges faced by cybercriminals has always been how to monetize the content they have acquired. Initially, many transactions were conducted person-to-person, on forums and private chat services. But with the rise in the scale of the theft came the emergence of credit card shops, account shops, and other marketplaces. The individuals responsible for the theft no longer had to worry about finding buyers — they could sell their stolen content to a marketplace for a lump sum or a share of the profit from sales.

In turn, markets like Slilpp, Joker's Stash, and Genesis Store made it easier for others to enter the underground economy. With shops like Joker's Stash, an individual no longer has to have technical skills to engage in credit card fraud. Criminals can download a plug-in following simple instructions provided by the shop, deposit a few hundred dollars, buy a few credit cards, and start making online purchases. In some cases, even the PII of the card holders could be obtained on the same shop, making it even easier to conduct the fraudulent transactions.

Some shops sell credentials for all sorts of accounts both generated or compromised by threat actors including bank accounts, cell phone accounts, online store accounts, dating accounts, and various other accounts that can assist in conducting online fraud. Threat actors can search by specific companies, domains, or simply types of credentials to help search through millions of available accounts. Moreover, threat actors can even acquire the digital fingerprints of compromised systems to help them masquerade as the victim device to help bypass anti-fraud measures implemented by legitimate companies.

It should also be noted that some shops sell credentials not only for client-accessed domains but also for corporate domains and VPNs from compromised systems and devices. This can be particularly dangerous as more sophisticated threat actors can use credentials obtained from employees to access internal systems and networks to perform social engineering, business email compromise, access escalation and other types of attacks. These types of attacks can frequently lead to breaches and the release and sale of databases obtained from the breaches, starting the cycle all over.

Mitigation Strategies

The variety in type of shops, marketplaces, and the accounts being offered for sale makes it difficult to suggest "one-size-fits-all" mitigation strategies. At a minimum we suggest the following strategies:

- Monitor shops and marketplaces for accounts relevant to your enterprise.
- Act on spikes in the number of accounts available in shops, as they may be indicative of a breach or a new TTP implemented by threat actors.
- Pay attention to any credentials for non-public facing domains as they can be used to facilitate further breaches.
- Enable MFA via SMS or authenticator applications such as Google Authenticator, Duo Mobile, FreeOTP, Authy, or Microsoft Authenticator to securely access devices.

Outlook: Enabling Blue Team's Response

In 2017, Gartner coined the term security orchestration, automation, and response (SOAR) to describe the emerging category of platforms born of incident response, security automation, case management, and other security tools. According to ESG research, 19% of enterprise organizations have adopted security operations, automation, and orchestration technologies extensively, 39% have done so on a limited basis, and 26% are currently engaged in a project to automate or orchestrate security operations.

With SOAR solutions, automation is used to programmatically execute a series of tasks without human intervention, and orchestration is used to integrate multiple, disparate security management and IT operational systems together to connect the automated tasks in a meaningful, actionable way.

There's one additional component that's required to make SOAR a realistic security solution: the data. This is where threat intelligence comes in — bringing timely, validated, and relevant threat data that is used to help make the best response decisions possible.

The key to making this all work is the IR workflows that tie together a SIEM solution such as Splunk, LogRhythm, or QRadar — alongside a SOAR solution such as DFLabs or SwimLane — with real-time threat intelligence such as Recorded Future. This requires security teams to look beyond the technology, extend their view beyond pure data processing, and develop a series of playbooks designed to tell stories of threats and attacks, and how to handle them using the collection of tools, services, and humans they have available. The workflows, if defined appropriately, enable security organizations to automate as much as possible and give humans the knowledge they need to validate responses and to pick up the slack if there are gaps in the automation.

The Importance of Threat Intelligence for MTtD and MTtR Metrics

In evaluating the value of SOAR solutions, two key metrics to apply include MTtD (mean time to detection) and MTtR (mean time to response). These numbers are key because many security breaches go undiscovered for months, giving hackers free rein and more time to access sensitive information. The faster you discover the breach, the less damage they can do.

And after a breach is discovered, it may still take a long time for IR teams to respond. They may be flooded with too much information, and they may lack the proper tools to conduct forensic analysis of breaches. This will delay their ability to pinpoint the cause of a breach and identify all the systems that have been impacted, which are essential to formally beginning the response process. The sooner the response, the better the breach can be contained.

Improving these two metrics is another area where threat intelligence has lately proven its worth. An IDC study found that organizations identified threats 10 times faster and resolved them 63% quicker after incorporating threat intelligence into their security processes.

The context provided by threat intelligence helps across all security functions; specifically in the case of incident response, it allows IR teams to evaluate alerts more quickly and confidently. For example, if an alert comes in flagging a suspicious IP address, it could be worth blacklisting or investigating further, or it could be a false positive — and it may take the IR team hours of manual research to come to a solid conclusion. And even then, their search may not be comprehensive. With a threat intelligence solution that automatically gathers and processes data from across the internet, this much-needed context is available in seconds instead of hours or days.

Download our new e-book to discover five ways you can automate security with intelligence to supercharge your security teams, tools, and processes.