CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

April 06, 2021

Cybercriminals Continue to Exploit Human Nature Through Phishing and Spam Attacks

Recorded Future®

Recorded Future analyzed current data from the Recorded Future® Platform, information security reporting, and other open source intelligence (OSINT) sources pertaining to phishing and spamming that facilitate threat actor campaigns. This report expands upon findings addressed in the report "Combating the Underground Economy's Automation Revolution", and will be of most interest to network defenders, security researchers, and executives charged with risk management and mitigation.

Executive Summary

In our March 2020 report "Combating the Underground Economy's Automation Revolution", we identified automated services and products that facilitate criminal activities. Phishing and spamming are attack vectors that often operate in tandem by bypassing network security settings, maintaining presence on targeted machines and networks, and extracting credentials for nefarious activities. This report dives further into phishing and spamming, identifying customized phishing and spamming kits and services within select dark web forums and analyzing widely used variants, and providing mitigation strategies to identify and deter phishing and spamming products attempting to intrude into your network.

Key Judgments

- Developers of phishing and spamming tools are creating kits and offering services that are customizable, automated, and designed to be user friendly to cater to non-technical and amateur users.
- Threat actors are using phishing and spamming services to bypass network security settings with the intent of deploying malware.
- Threat actors are discussing specific phishing and spamming variants on different forums, with "Multithread WebMailer GoMAIL Pro Edition" and "uPanel" being widely advertised and discussed.
- Spamming and phishing as a service (PhaaS) are popular topics of discussion between threat actors on forums. Some commonly discussed tools include Evilginx and MoneySpamBot.

Background

Once threat actors have obtained credentials from database breaches, or sometimes by simply conducting Google queries, their next step is to target victims with large-scale phishing and spamming techniques where cybercriminals, if successful, will gain unauthorized network and personal account access. As a result of many of the targeted systems or devices being protected to some extent by antivirus software, which may recognize, flag, or block phishing and spamming attempts, threat actors have created homemade tools to bypass security measures.

As the number of phishing and spamming attacks increase, more threat actors are using innovative attack vectors to deploy new variants of malware. Some of these threat actors do not possess the technical expertise or are not dedicated to maintaining their own phishing or spamming tool, instead turning to more technically savvy threat actors to develop, maintain, and offer these services. Given these needs, developers of automated phishing and spamming tools have capitalized on the market demand for these services by providing customized products.

Phishing

Phishing remains a popular attack vector for threat actors to conduct social engineering attacks, deploy malware, harvest credentials, conduct business email compromise (BEC), and gain further access into targeted networks.

Phishing remains effective because it exploits the human factor in a given system, and threat actors are able to adjust and improve their tactics to increase the chances of a victim opening a phishing message that contains a malicious file or link. Some of these tactics include posing as a trusted brand (a secondary threat to retail businesses in the form of brand damage), using urgency to make the victim think they need to act quickly or face a negative consequence, or impersonating someone within their organization, such as an executive, to request funds and wire transfers.

In addition to these more traditional phishing methods, threat actors deploying this attack vector continue to update their tactics and incorporate newer technologies to facilitate their activities. Threat actors used phishing emails to send weaponized disk image files (ISO/IMG) to victims that were used to later deliver malware, including remote access trojans.

COVID-19 Phishing Lures

Playing on public fears and thirst for information, threat actors frequently incorporate major events into their techniques, creating lures that are timely and relevant to their target audience. For example, since early 2020, cybercriminals have continued to exploit the COVID-19 pandemic to consistently target multiple sectors with phishing lures designed to capitalize on the uncertainty it has generated. The COVID-19 pandemic has had major impacts on the cyber threat landscape throughout 2020 and into early 2021. Threat actors have been observed propagating malware by employing references to the COVID-19 pandemic in various attack vectors, including COVID-19-themed lures in phishing emails and SMS messages, malicious mobile applications, and other techniques. In Q2 2020, phishing attacks were the second most referenced cyber threat within the Recorded Future Platform, with over 45,000 references within the past quarter. Reports of phishing events targeted nearly all industry verticals and were generally consistent over the quarter, with a few spikes. Of those spikes, 5,255 references consisted of phishing attacks with COVID-19-themed lures. Some of these attacks include phishing attacks delivering a malicious update to NetSupport Manager that dropped NetSupport RAT and abusing Google Firebase Storage.

Threat actors use COVID-19-themed attacks like sending phishing emails with COVID-19 lures to deliver Trickbot, injecting malicious code into COVID-19 maps and contact tracing apps, and more. As the pandemic continues to evolve and public concerns evolve along with it, threat actors will likely identify more opportunities to exploit the public's concern and need for immediate updates on the pandemic, particularly when and where vaccines are available.

In addition, the pandemic has created a shift to remote work for organizations across the globe. We believe that the greatest risk to organizations in terms of remote work comes from threat actors targeting VPN and remote access tools with weak or compromised credentials. Because remote working environments inherently grant users remote access to closed networks, threat actors pursue legitimate credentials more aggressively. Use of legitimate credentials decreases the likelihood that intrusion activity would be quickly detected. While vulnerabilities to these technologies still present a threat to remote work, vulnerabilities in VPN and remote access tools themselves are not necessarily the greatest organizational risk.

For many organizations, the digital transformation they had planned to implement over the next several years has happened nearly overnight. While the change in enterprise network baselines, operating schedules, and security operations are in flux, threat actors are seizing on this period of transition. On April 21, 2020, the Federal Bureau of Investigation (FBI) warned of an ongoing COVID-19-themed phishing campaign targeting US healthcare providers with malicious attachments. In addition, threat actors have been using phishing attempts to take advantage of the technology used to allow business continuity during this shift to remote work such as Zoom and WebEx.

Phishing Kits

Phishing kits are designed for ease of use. Social engineering attacks combined with customized tools like phishing kits make phishing attacks automated and uncomplicated. Once a kit has been purchased or created, the threat actor typically installs it on a remote server, whether by purchasing it, compromising legitimate content management systems, or via exploits like SQL injection bugs. When a kit has been set up, they install a Simple Mail Transfer Protocol (SMTP) mailer so recipient lists can be emailed in bulk. If the user inputs their personal data on a phishing page they then typically get redirected to the legitimate website. To further discourage user suspicion, the phishing kit may automatically log the user onto the legitimate website using the username and password that the victim submitted on the phishing page. Using source code from phishing kits, stolen information is sent back to a scammer's remote location through email or File Transfer Protocol (FTP) connection, or it may be directly stored on a text file located on the phishing server.

Additionally, to prevent unwanted access to their phishing kits and discovery, attackers use a number of techniques to hide their activities, including .htaccess files with a list of blocked IP addresses related to bots from search engines and security companies and PHP scripts which checks to see if remote IP addresses are permitted to access the phishing pages scripts which are often included in kits.

In early February 2021, Ukrainian police forces arrested an unidentified man on charges of developing and advertising one of the most advanced and widely used phishing toolkits on the dark web. The threat actor is suspected of authoring the phishing kit named uPanel, sometimes also referred to as U-Admin. U-Admin is a control panel for receiving logs from phishing kits, and controlling victim interaction. U-Admin is also used with injections, which are snippets of code that are injected into a victim's browser, enabling the attacker to gather more information from their victims. The Ukrainian Ministry of Internal Affairs was able to confirm that uPanel had more than 200 active customers based on data they obtained after seizing computers, laptops, and smartphones from the suspect's residence. Ukrainian authorities believe that the phishing kit had been active since 2015 and used in phishing operations that caused tens of millions of losses, in US dollars, to financial institutions in at least 11 countries.

We believe that the creator of uPanel was the threat actor "kaktys1010", a member of the forums Exploit and XSS as well as the currently defunct Infraud forum. The threat actor was a developer of Windows and Android web injects and fake web pages with and without SMS/token interception, and was also a creator and operator of the website KTS and offered a wide range of HTML web injects, designed to target multiple banks and financial organizations worldwide, that are divided into the following categories:

- Android web injects
- Fake web pages
- Dynamic web pages
- Static web pages
- TrueLogin web pages
- Injects
- Uncategorized

The price range of the web injects varies from $60 to $500 USD.

The threat actor was a developer and seller of Android web injects and phishing pages crafted specifically for social media and messenger platforms with payment card grabber functions. For instance, on April 11, 2016, kaktys1010 released a web inject pack that targeted Facebook, Instagram, WhatsApp, Viber, Skype, and Google Play, and cost $450 USD. The threat actor embedded the phishing generator function in their web injects, allowing attackers to change the color, font, and location of the elements on the phishing web page, as well as other properties. Recorded Future previously conducted an in-depth report regarding banking web injects and kaktys1010.

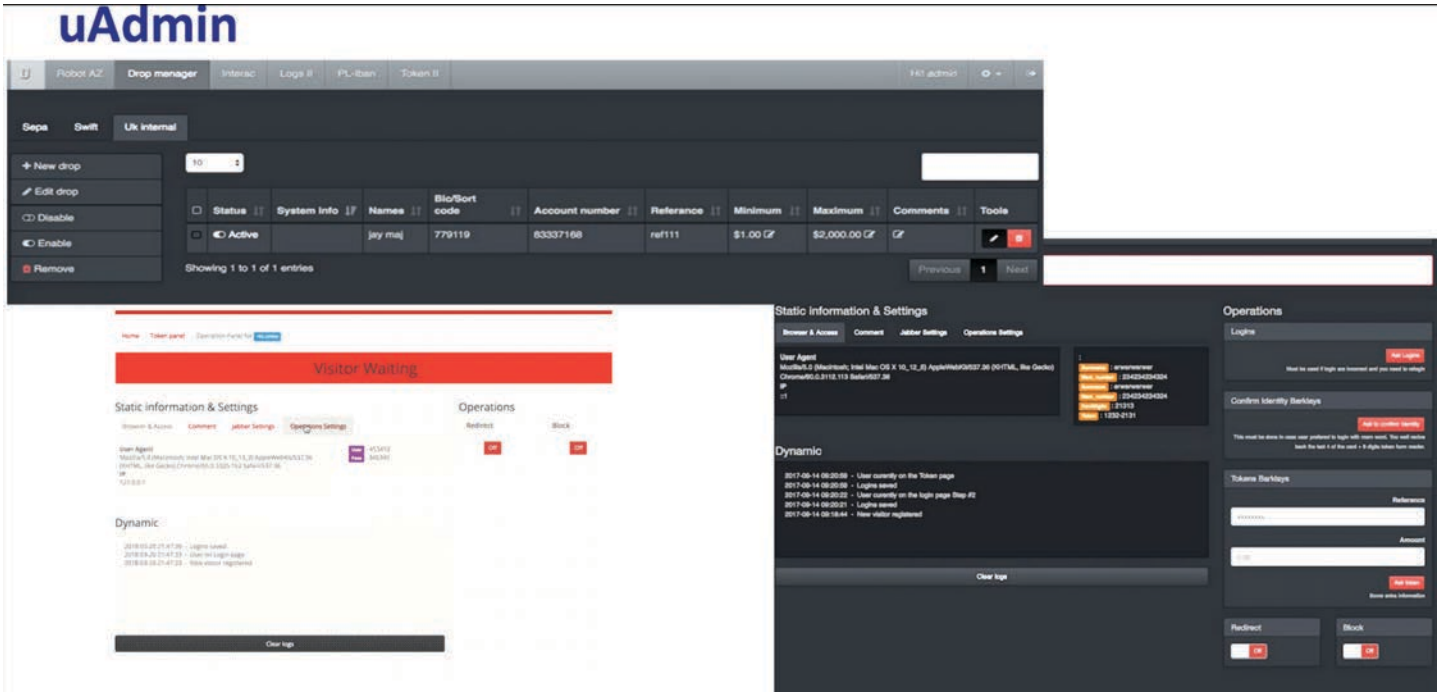

Figure 1: uAdmin panel developed by Kaktys1010 (Source: Exploit forum)

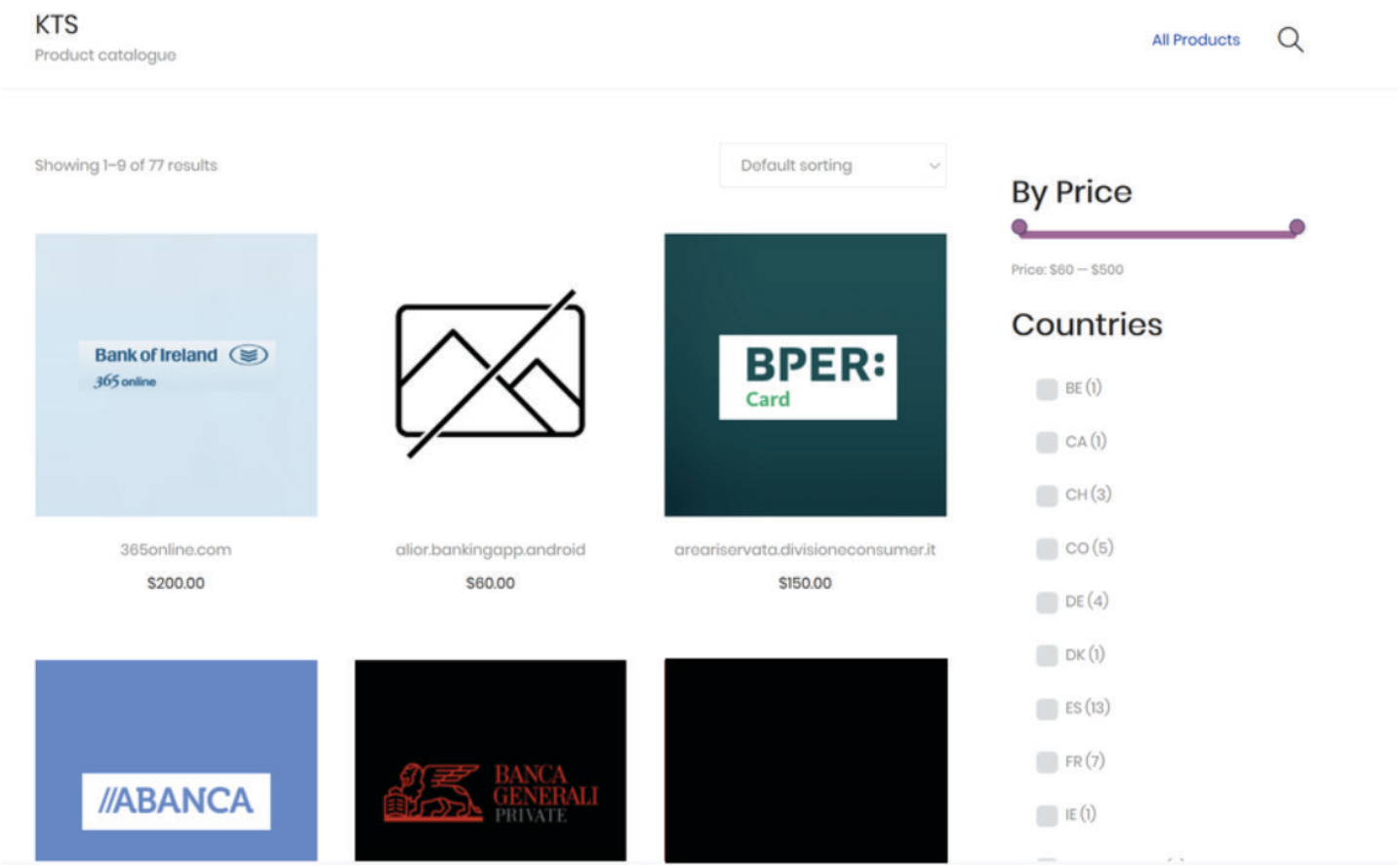

Figure 2: Image of the uPanel store hosted on the dark web (Source: KTS)

kaktys1010's web injects can be controlled with an admin panel called "uAdmin" (universal admin). The admin panel is linked to the following plugins:

- Log parser
- Event logger
- Virtual Network Computing (VNC) — provides connection to the botnet API via VNC and SOCKS.
- Token interception
- Victim tracker
- Additional framework plugins

After the arrest in early February 2021, kaktys1010 was banned on the forums Exploit and XSS, his account was deactivated by the forum administration, and the website KTS, which he operated, is currently defunct.

Phishing as a Service

Across the dark web ,threat actors are offering a phishing-as-a-service) PhaaS (model for cybercriminals who are involved in the phishing business ,which includes development of phishing or fake pages ,online technical support ,and regular updates for customers .We observed a number of notable PhaaS-related events across dark web sources during the research period.

On August ,2020 ,3 the threat actor" John_Malkovich "on the forum Exploit advertised PhaaS .According to the threat actor ,their phishing pages are 100% identical to originals and allow collecting login ,password ,session cookies ,and other information .The service provider stated that their phishing simulators are supported by built-in developed software platforms that facilitate phishing campaigns .The seller was offering their phishing services against several organizations for a monthly rental price for) 500$ with a free one-day test.(

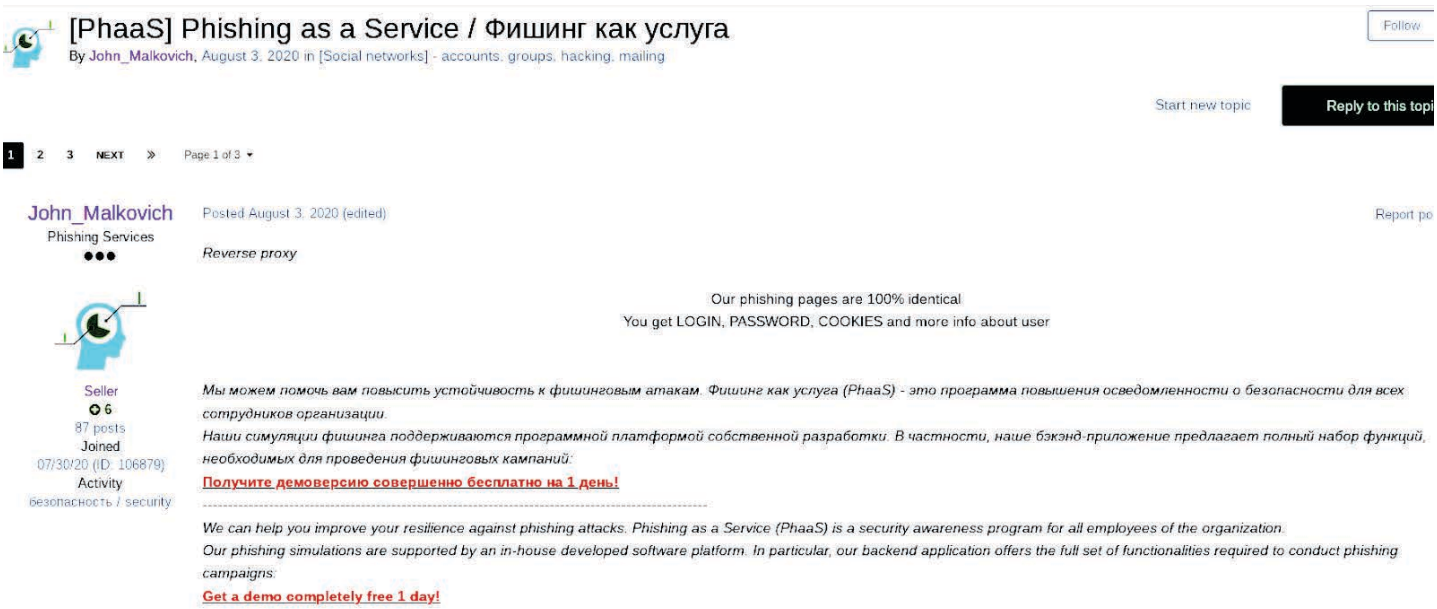

Figure 3: PhaaS advertisement by John_Malkovich (Source: Exploit forum)

The threat actor is offering advanced technical functionality for Binance cryptocurrency exchange for .2,000$ According to John_Malkovich ,the phishing kit performs the following operations:

- 2FA bypass
- Anti-bot protection
- Advanced collection of session information (logins, passwords, and cookies)
- Telegram notifications
- Creation of multiple phishing pages per domain
- Geolocation filtering
- Online support
- Phishing page manager module

On November 27, 2020, the threat actor "Consistentcode00" offered an advanced phishing service targeting organizations for a monthly rent of between $500 and $3000.

The threat actor stated that their phishing kit is based on the modified Evilginx man-in-the-middle framework used for phishing credentials and session cookies of any web service, which can successfully bypass multi-factor authentication. Consistentcode00 is looking for cooperation with experienced spammers.

Spamming

Spamming campaigns can continue to harass businesses and individuals through fraudulent requests to transfer funds, and require little technical sophistication to conduct. Social engineering and finding good "leads" for criminal campaigns to be orchestrated are two of the primary factors for success by a malicious threat actor. Unique methods are either rarely discussed by cybercriminals or are eventually sold at a price above those of other methods of spamming that are advertised by competitors. In addition to services surrounding lead generation, spammers are typically able to obtain email information through the following methods:

- Using software to generate email addresses
- Enticing people to enter their details on fraudulent websites
- Hacking into legitimate websites to gather user details
- Buying email address 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

Spam, through a combination of email, SMS, and messaging platforms, was still one of the primary methods of malware and phishing distribution in 2020. According to Mimecast, a review of their global customer data revealed that impersonation fraud increased by 30% in the first 100 days of the COVID-19 pandemic, with 60% of respondents' organizations being impacted by malicious activity that spread from employee to

employee. Threat actors continued to take advantage of more tolerable security mechanisms in SMS to distribute URLs or malware samples on a regular basis (both within criminal sources as well as malware campaigns that appear to proliferate through legitimate platforms such as social media accounts).

We have also consistently observed threat actors in the past year discussing key components of successful spamming activity, including the vital role of finding promising targets through "leads". Cybercriminals show a high awareness that many supposed leads for spamming activity are useless for effecting data theft, and therefore have come to expect a level of competency when sampling a service advertised within an underground source. Requests such as this continue to suggest that databases containing large volumes of information, such as those that include only email addresses or that lack a specific company focus, are worthless to cybercriminals interested in spamming activity.

Fresh leads may independently appear for sale within an underground source with no reference to spamming activity as seen in the example above in Figure 4. Despite this, advertisements such as this are likely to be of interest to those attempting to inundate a particular target with correspondence possibly containing malicious links more characteristic of a phishing email. The low price value in the example above ($25) is likely to fit the budget of any aspiring cybercriminal entity. Leads that were reported to have been derived from a targeted entity or industry typically were available for higher prices in comparison, as seen in the example below in Figure 5, which originates from the same criminal source seen in Figure 4. While this price may also factor in the sheer volume of information for sale, it was consistent with other more expensive criminal advertisements related to phishing kits or tools designed to target a specific entity rather than tools less tailored to entice a particular end user to engage with them.

Advertisements for other forms of criminal activity, including business email compromise operations, continue to promote custom phishing pages designed to achieve success against specific entities. Threat actors have claimed that scam pages normally require the use of tools like "cpanel or smtp" to set up convincing web infrastructure and that good leads would be difficult to find manually. This very likely indicates that new spamming campaigns or tools advertised within underground sources will likely have to be easier at times, not more complex or technically demanding to use, to achieve greater sales. Additionally, the exposure of company email addresses across multiple industry verticals in data dumps, dark web forums, extortion sites, and paste sites has very likely increased the threat of malspam or phishing campaigns to individuals whose information has been referenced in these dumps.

Requests related to the sale of tools designed to support fledgling spam operations as well as advertisements recruiting potential partners continued to persist throughout 2020 across both high- and low-tier dark web communities. SMS spamming methods, in particular, often catered to threat actors with no familiarity on the topic, as seen in Figure 6 below, attempting to entice potential buyers by informing them that "no skills" are required.

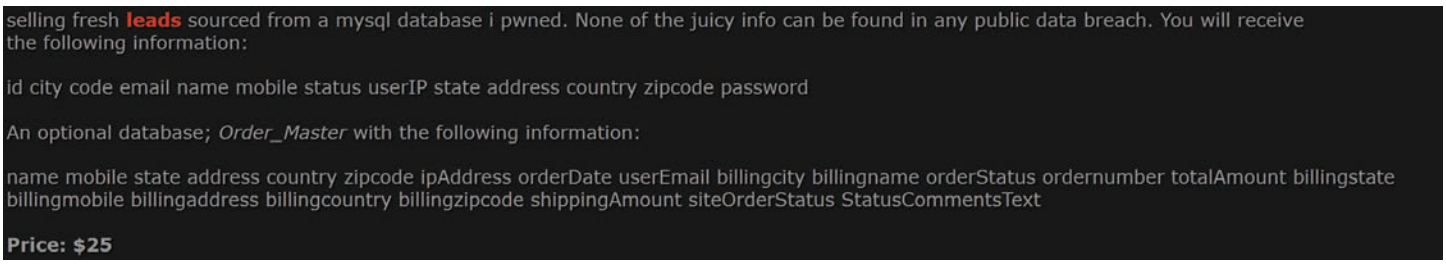

Figure 4: Underground advertisement for fresh leads originating from privately owned database (Source: Club2CRD)

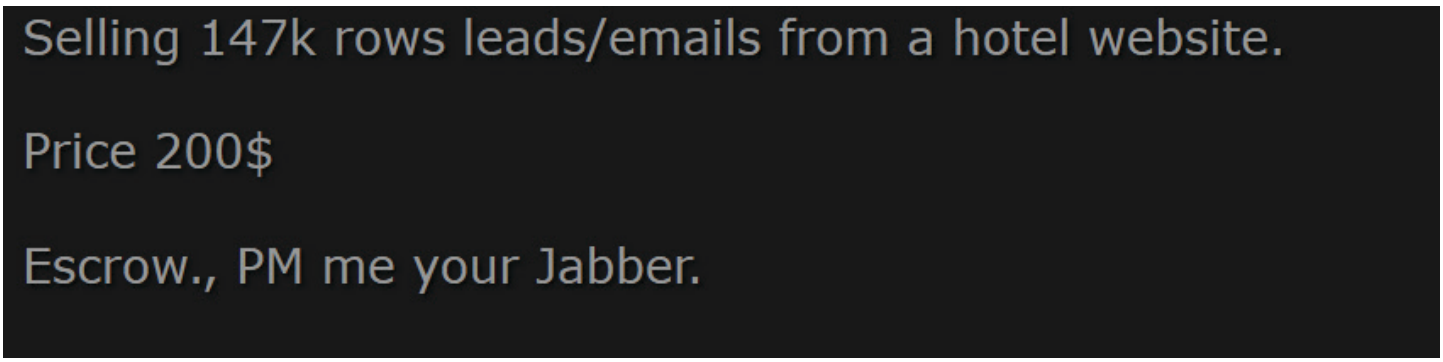

Figure 5: Underground advertisement for leads associated with the website/domain of a hotel chain(Source: Club2CRD)

NEW SMS SPAM METHOD WORKING NOVEMBER 2020
YOU WILL RECEIVE THE SPAM METHOD AND 1 FREE SPAMMING PAGE

- No skills needed
- No phones needed
- No sim needed
- No bs
- All you need is a computer

You will learn:
- How to send sms witouth beeing blocked for canada
- How to host properly website for spam
- How not to get banned
- How to add ssl certificate to website

PROOF AVAILABLE IF YOU HAVE MANY SIM CARDS AND PUT DEPOSIT I will spam them for you.
I do not offer spam service. simply proof. I do not have time to spam full list for you this is why i sell method.

Figure 6: Underground advertisement for SMS spamming method catered toward low-tier cybercriminals (Source: CanadaHQ)

Bulletproof hosting services (BPHS) provide secure hosting for malicious content and activity and assure anonymity to threat actors have increasingly appealed to various criminal entities including those operating spamming services. The hosting service advertised below in Figure 7 attempts to appeal to a variety of use cases as being "spam friendly", capable of performing the bulk of the setup for threat actors who may be unfamiliar with the concept of creating infrastructure for their operations capable of withstanding potential service disruptions or the from grabbing the attention of law enforcement entities. Services such as this have recognized the demand for spammers to use social media platforms and have made attempts in some cases to advertise their capability to persist on these platforms as a core feature. Based on these common use cases, bulletproof hosting services in 2021 are likely to continue to include the distribution of phishing or spam messaging.

Several spamming-related tools or services advertised within the criminal underground over the past 6 months that were favorably received by other members included the following:

Figure 7: Advertisement for "spam friendly" email servers (Source: Exploit)

Multithread WebMailer GoMAIL Pro Edition is an email spamming kit released by the threat actor "Prospere" on the forum Exploit on November 17, 2020. According to Prospere's statement, the spamming kit completely emulates real PC and human actions, which allows attackers to increase the life and number of emails sent from consumables many times and to reach a victim's inbox. The Multithread WebMailer GoMAIL Pro Edition tool is suitable for mass mailing (including attached files) in public inboxes with a high inbox rate, collecting responses and answers and sending spam using email databases. The threat actor stated that a lifespan of a typical spamming account is from 1 week to a month. A daily spam limit is up to 500 emails, but usually ranges from 100 to 150 emails.

The following technical specifications were provided by Prospere:

- Multithreading
- Human emulation
- Save machine fingerprints (operating system, web browser, proxy servers, and so on)
- Save and work with profiles and cookies
- Support SOCKS5/HTTP protocols
- Send email through TO, CC, and BCC modes
- Work with multilingual Google accounts
- Spam through various Google services such as Google Docs, Slides, Calendar, and so on
- Craft spam text and topics
- Support malicious links and attachments

The spamming tool is available for rent:

- A monthly price for $680
- A weekly price for $250 (SOCKS5 proxy servers included)
- 1,000 spamming accounts for $280
- A monthly rental for a server for $150
- A module for receiving and modifying replies for $100 (the second month is for $50)

The threat actor is ready to provide a free 5-hour test via their servers and proxies.

Mail:pass is a service promoted on Exploit by the threat actor "Moriarty221B" since 2018 and designed to supplement brute force and spamming threat operations. The service regularly uploads fresh information pertaining to US or EU entities, with database information being listed as available in "MAIL:PASS format with IMAP/POP3 access". Mail:pass has been prominently advertised on Exploit on a regular basis via a banner on the forum, alongside other popular criminal sources such as Genesis Store. The service also promotes the sale of mail access lists for the specific purpose of disseminating spam messaging, with flexibility in selecting domains a threat actor may be interested in emulating. The thread promoting Mail:pass has continually been updated by Moriarty221B into 2021, informing other forum users when new valid information becomes available for purchase.

Other prominent features associated with the service were listed to be as follows:

- Regular database updates (1 to 2 times per week)
- Can review databases for specific information upon request
- 24/7 customer support

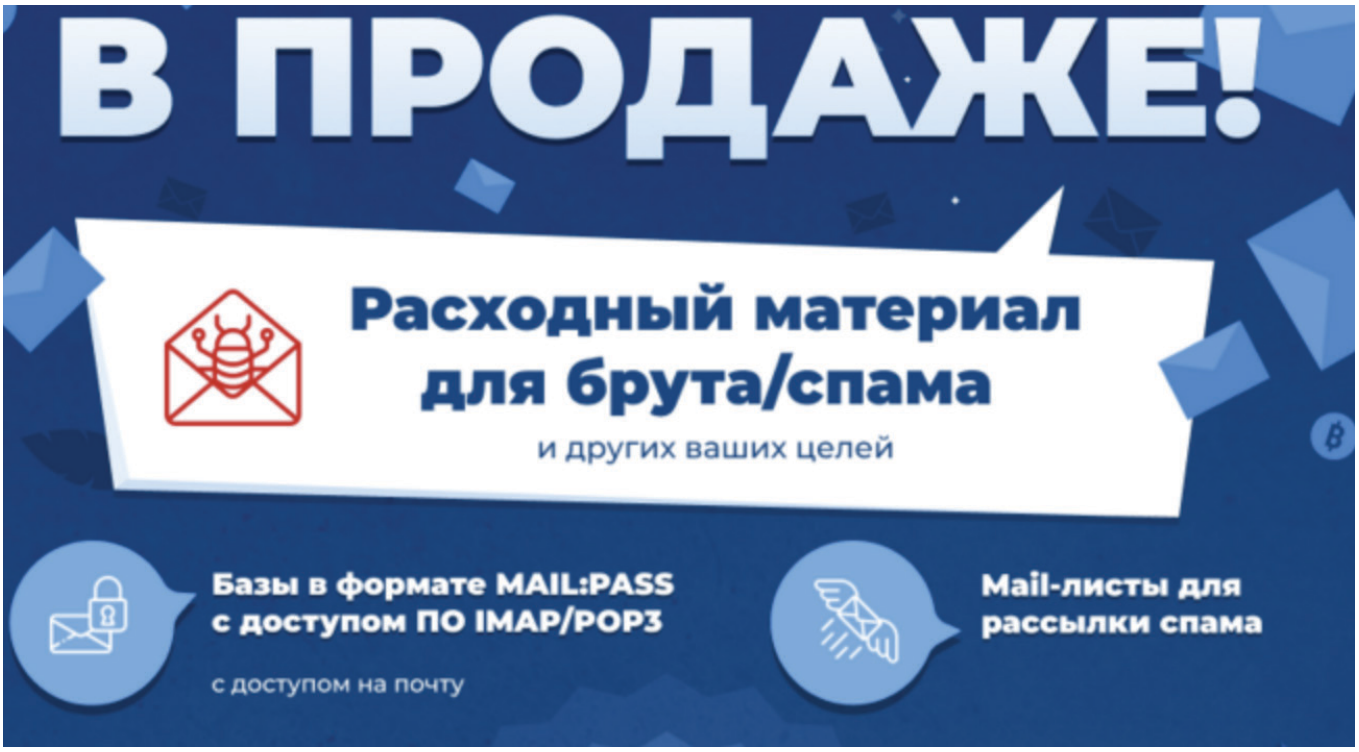

Figure 8: Mail:pass banner promoting mail access lists for spamming (Source: Exploit)

[Translation: FOR SALE! Consumables for brute/spam and other things Bases in the MAIL:PASS format with access via PO IMAP/POP3 Mail-list for spam distribution with access to mail]

MoneySpamBot refers to a spam botnet rental service with HTML support advertised by "Joynses", a member of XSS forum, since December 2020. A standard license for the service enables threat actors to regularly disseminate spam correspondence and optionally integrate with other messenger platforms or API regarding the spam. The spam botnet can be rented on a monthly basis and has 2 available rental options:

- $350 per month for a Standard license
- $850 per month month for a Pro license

The Pro license advertisement includes several additional optional features, including:

- The ability to monitor controlled BTC wallets
- Sending file attachments in a message
- The ability to monitor responses from recipient mailboxes
- Enabling sender spoofing options (depending on the domain being emulated or targeted)

Joynses has received positive feedback on XSS related to other services the threat actor has historically been observed advertising, including the sale of network access to targeted organizations as well as Avalon Stealer, an infostealer written in C# and first observed on July 7, 2020. Based on the underground advertisements and the decompiled code published on GitHub, the stealer harvests credentials and sensitive information that would likely be appealing to threat actors compiling information for spamming-related purposes from browsers, email, FTP clients, messaging apps, VPN, RDP files, cryptocurrency wallets, and other local files.

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 includes but is not limited to password expiration and complexity.
- Deploy a web filter to block malicious websites.
- Require encryption for employees, especially employees working remotely. This includes whole-disc, 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.

Using the Recorded Future Platform, clients can identify phishing and spamming widely used by threat actors to target their brand, which may indicate planned phishing or spamming attacks against them. Setting up Platform alerts allows a user to monitor for phishing updates and tactics, techniques, and procedures (TTPs) being used by threat actors.

Outlook

In 2020, phishing and spamming presented itself as a major threat across all industries and saw a major increase beginning in March 2020. Online users still have difficulty telling the difference between a real website or email and a nefarious one.

Cybercriminals will likely continue to use phishing and spamming because of the success they have had with gaining unauthorized access to user accounts and the profits they make from selling customized tools across dark web sources. This practice will continue to threaten companies and individual users until improved password hygiene standards and security measures are implemented.

Opportunism has been a consistent hallmark of cybercrime, and cybercriminals will likely continue to take advantage of human nature, such as by putting pressure on victims to relinquish private information and preying on target's gullibility and kind nature as the COVID-19 pandemic progresses. We believe that an increasing number of phishing operators, spammers, and fraudsters will exploit the news and climate surrounding the pandemic. On the technical side, COVID-19 brought about a rush of phishing attempts using COVID-19 lure documents and tailored malware. Both the domain registrations and malware/phishing campaigns are likely to continue to follow the general curve of the pandemic.

About Recorded Future

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.