CYBER
THREAT
ANALYSIS

Recorded Future®

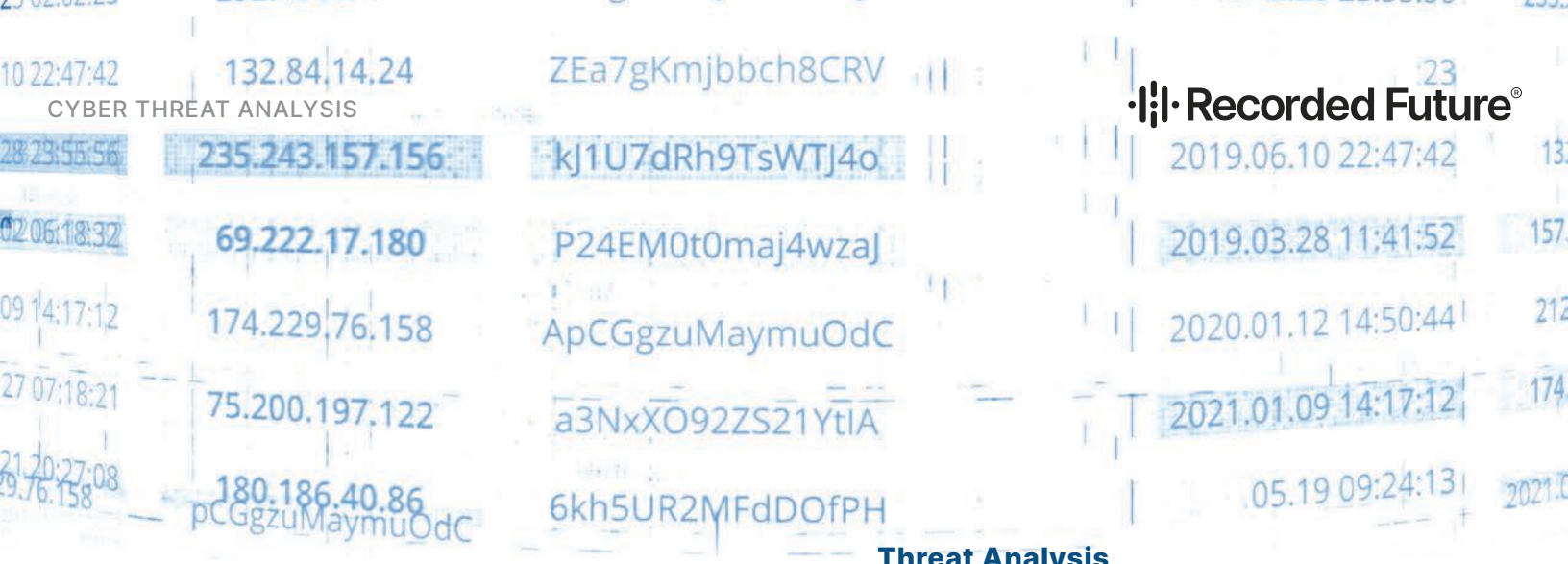
By Insikt Group®

November 12, 2021

THE BUSINESS OF FRAUD:

Botnet Malware Dissemination

Recorded Future®



Recorded Future analyzed current data from the Recorded Future® Platform, as well as dark web and open-source intelligence (OSINT) sources, to review botnets ("not-auto buy" botnets) that facilitate nefarious activities by threat actors. This report expands upon findings outlined in "The Business of Fraud: An Overview of How Cybercrime Gets Monetized". It will be of most interest to anti-fraud and network defenders, security researchers, and executives charged with security and fraud risk management and mitigation.

Executive Summary

Botnets are networks of computers infected by malware (such as computer viruses, keyloggers, and other malicious software) that are controlled remotely by online threat actors to garner financial gain or to launch attacks on websites or networks. When a computer is infected by a botnet, it communicates and receives instructions from command-and-control (C2) computers located around the globe. Many botnets are designed to harvest data, such as passwords or phrases, Social Security numbers (SSNs), credit card numbers, addresses, telephone numbers, and other personally identifiable information (PII). The data is then used for nefarious purposes, such as identity theft, credit card fraud, spamming or phishing, website attacks, and malware distribution.

Key Judgments

- While IcedID has surged in spam volume, TrickBot and QakBot have shown much more consistency in the volume of spam and infection traffic pertaining to fraud purposes since Emotet's takedown.
- Financially motivated threat actors, nation-state actors, and APTs in various international regions will continue to use botnets for fraudulent purposes to attack targets.
- Underground forum courses on how to best use botnets will remain popular among threat actors for the foreseeable future, particularly as the world becomes increasingly digitized.

Threat Analysis

In a report published by the International Data Corporation (IDC), researchers predict that "by 2025 there will be 55.7 billion connected devices worldwide, 75% of which will be connected to an IoT platform". According to a recent report conducted by Barracuda Research in September 2021, bots make up nearly two-thirds of internet traffic, with malicious bots making up nearly 40% of all traffic. In today's cyber threat landscape, the term "bot" is used widely to describe automated processes for both legal and malicious purposes, with examples of these terminologies below:

- Spambot: An application designed to gather email addresses from a variety of websites, adding them to lists to send unwanted emails.
- Ticket/auto-buy bot: an application that automatically buys commodities (such as tickets or retail items), especially commodities that have limited or special releases. The operators of these botnets are usually motivated to resell items at higher prices on the secondary market.
- Social media bot: an application that specifically operates on social networks to post and amplify messages, infiltrate groups, create fake accounts, collect postings, and more. Russian agents successfully deployed social media bots before the 2016 US Presidential election to stir resentment and spread disinformation.
- Botnet: an infected machine that is controlled by a threat actor via a command and control (C2) serve with the intent of using the machine (usually with other infected machines) to launch network disruptions (DDoS), injection malware, harvest credentials (as in Genesis Store listings), and other nefarious purposes.

For this report, we will focus on how cybercriminals use botnets to facilitate their fraudulent activities.

Figure 1: Comparing reported botnet activity since Emotet's takedown (Source: Recorded Future)

Background

Cybercriminals, as well as nation-state threat actors, have continued to demonstrate the flexibility and dynamic aspect of conducting botnet operations that leverage routers and other equipment to perform unconventional tasks such as rendering devices inoperable or using them to disseminate malware strains specifically designed to support financially-motivated fraud activity.

Regarding cybercriminals, these threat actors used Emotet, arguably one of the most popular botnets created until it was disrupted by law enforcement in a January 2021 operation and eventually dismantled in April 2021, to download third-party banking malware such as TrickBot, IcedID, and Gootkit. Customers of botnets that cater to cybercriminal entities that specialize in forms of fraudulent activity include operators of infostealer trojans, business email compromise (BEC) groups, and ransomware gangs. Additionally, tutorials for the development and support of botnets specifically designed to execute malware with functions specifically repurposed to conduct fraudulent activity such as logging keystrokes (keylogging) remained plentiful within the criminal underground throughout 2020.

The figure above breaks down the botnet activity of the most active botnets since Emotet's takedown. After the takedown in January 2021, the use of the other four main botnets has increased at varying levels for campaigns targeting victims.

Outside of basic tutorials or methods for the development of a botnet with limited features, statistics across the security community in 2020 continued to reveal that more prolific strains of malware commonly associated with malicious botnet activity remained the most popular strains affecting all industry verticals by the end of the year.

The successful law enforcement takedown of the Emotet botnet has left a void in the loader space. Despite frequent breaks, the botnet was one of the most prolific and profitable threats in 2019 and 2020. While a large number of malware families use spam and loaders to generate infections, only some of them represent a threat to enterprises because of their capabilities, their follow-on infection chains to deploy ransomware and their sheer volume. This eliminates common keyloggers such as AgentTesla or Formbook and narrows the focus to 4 main botnet families: TrickBot, QakBot, IcedID, and Dridex. There are also specific distribution tools and methods that these botnets use to supplement or substitute their spam campaigns.

Although law enforcement succeeded in taking down the Emotet botnet, Emotet and TrickBot were suspected to have been operated for a time by different threat actor groups. However, TrickBot's operators have used Emotet as a dropper/loader for their own malware variant. The hosts are being distributed to brokers and used as initial access vectors for corporate network compromise and potential distribution of ransomware variants, including the Ryuk ransomware variant. 2 malware strains that

have continued to be observed working in tandem via the operators of Emotet in 2021 include TrickBot and QakBot, with the latter suspected of having replaced TrickBot for a time given the shift in payloads being deployed onto victim systems to steal banking information to the appeal of criminals conducting fraud.

Considered to be the successor to the infamous Dyre banking trojan, TrickBot banking trojan leverages multiple attack vectors, including redirection attacks and web injects, to attempt to steal information from financial institutions and initiate fraudulent wire transfers. The primary methods used by threat actors to distribute banking web injects continue to be phishing and exploit kits, with injects often flourishing within cybercriminal communities that offer customized options catered to threat actors attempting to target a specific company. Additionally, administrative panels associated with web injects sold within underground sources have historically been observed promoting features such as the inclusion of plugins to connect with botnet infrastructure.

Threat actors continue to generate profit from the development or sale of malware strains that incorporate keylogger functionality to steal information of interest, particularly on low-tier forums that likely attract a broader audience. TrickBot has previously been co-opted to distribute ransomware and other banking trojans, using the botnet formed by a large number of infections. Despite the United States Cyber Command and the security industry's attempted disruptions of the TrickBot botnet, the controllers associated with the malware have continued to remain resilient.

Botnets and Distribution Methods

After Emotet's takedown, QakBot and TrickBot had initially surged to a large portion of detections globally. Currently, IcedID and Dridex are the most prolific botnet threats. Each of them has been observed acting as precursors to ransomware: IcedID was linked to Egregor deployments, TrickBot attributed by CrowdStrike to the same threat actors that authored Ryuk and Conti ransomware families, Dridex has been tied to DoppelPaymer, and QakBot has deployed ProLock and DoppelPaymer.

TrickBot

TrickBot is a modular banking trojan that has been active since 2016. TrickBot is typically delivered via phishing campaigns and then executed in memory with additional plugins being downloaded at a later point. TrickBot leverages its plugins to gain deeper network access, further propagate its spam, and issue multiple attack vectors for monetization including web injects, password stealing components and the initiation of fraudulent wire transfers.

TrickBot's developers continue to modify and update the backdoor, components, and infrastructure, specifically after takedown efforts in the fall of 2020. TrickBot's operators have split their infrastructure into 2 distinct branches. Each branch was built by distinct server types in early 2021, before using identical but distinct C2 nodes beginning in March 2021. Our visibility indicates the original branch continues to service TrickBot clients, while the secondary branch has been only used for in-house TrickBot operations. The shift is likely a resiliency effort; TrickBot's operators can continue spamming operations via a secondary botnet branch, even if the more used one gets taken down or blocked based on the volume of infections.

TrickBot is a sophisticated malware variant, offering operators various evasion techniques, as well as different methods of spreading, and a large number of capabilities to generate revenue for criminal users. One of the primary functions of TrickBot (similar to other banking trojans) is to lift credentials and other sensitive login-related data appealing to financially motivated threat actors using methods such as web injects and a keylogging function. As database breaches and login credentials with passwords have become widely marketed by threat actors, keylogging as a standalone attack vector to harvest credentials through the deployment of botnets has become less relevant. Information of interest to threat actors includes usernames, passwords, personal identification numbers, and possibly answers to security questions. The role of the malware acting as a loader to download additional payloads of malware cannot be overstated.

While TrickBot has made efforts to harden its infrastructure, it has decreased the volume of spam campaigns. TrickBot has used both BazarCall and Campo distributions as mentioned above, but also relies heavily on its own spam campaigns to generate infections. TrickBot's spam operations are often run by affiliates, and TrickBot's operators provide them with unique malware samples with embedded G-Tags to track how effective the affiliate was to help determine profit sharing.

QakBot

QakBot is a modular, information-stealing trojan that was first discovered in 2007 and has recently experienced a resurgence. QakBot is typically delivered via phishing campaigns and then executed in memory with multiple plugins being loaded from the malware's resource section or downloaded. QakBot injects itself into a running process, typically explorer.exe, to evade defenses. QakBot has multiple modules to help monetize their intrusions, including those for propagation, web injects, email collection, and other data theft. One of the main capabilities being leveraged by threat actors deploying QakBot is its ability to load and run additional malware.

QakBot is linked to several affiliates with varied naming conventions. The most prolific of these is TR, which, unlike others, does not get appended with incrementing numbers for each new campaign. TR-based spam uses hijacked email threads from prior victims, and is identified with the beaconing URI structure, which is typically "/ds/<DDMM>.gif". TR is used to conduct phishing campaigns for other malware families including IcedID and has been used to drop Cobalt Strike in DoppelPaymer-linked intrusions.

The TR distributor has been linked to the use of the EtterSilent (aka SilentBuilder) malicious document builder, which is also used by other criminal syndicates, to build malicious Excel 4.0 macro spreadsheets for distribution.

SQUIRRELWAFFLE is a lightweight loader first deployed at scale by the TR distributor in September 2021. Shortly after what was a likely test phase in early September, SQUIRRELWAFFLE saw international distribution via multi-language spam campaigns starting September 20, 2021. These campaigns returned to TR's reliance on the EtterSilent document builder. The loader directly dropped Cobalt Strike Beacons and QakBot modules; the latter was used to facilitate further spam operations.

QakBot regularly cycles the overlaps in affiliate infrastructure, as shown by data from the configuration file included in the malware's resource section. At the time of analysis, the TR and Obama affiliates shared 95% of the same infrastructure, distinct from the 95% infrastructure overlap between the Biden and Clinton affiliates. The Abc affiliate operated on a relative island, with only 8% overlap with the Biden and Clinton infrastructure. Previously, TR and Biden affiliates had substantial overlap in infrastructure; this cycling is likely to improve resiliency across the operation.

Dridex

Dridex is a banking trojan that first appeared in 2014, which uses web injects, keylogging, and email stealing functions to monetize infections. Different communication modules can be loaded by the malware to facilitate VNC, peer-to-peer (P2P), or other alternative communication messages. Dridex is typically distributed via phishing campaigns as a malicious attachment or link. The malicious attachment often contains macros that once opened reach out to a C2 server to download the actual Dridex malware. In some instances, Dridex is embedded in the attached file and will be extracted when opened by the user.

Dridex had 4 active affiliates, at the time of analysis, all of which use a different configuration file embedded in Dridex's main payload. The affiliate IDs are regularly rotated or aged off, making it difficult to track customers or methods used for distribution over time.

IcedID

IcedID, also known as BokBot, is a banking trojan that has been active since 2017. The malware has embedded functionality to spread to other hosts on the same internal network and uses web injects with redirection, as well as cookie and credential stealer functions for monetization. IcedID is often delivered using phishing, with Microsoft Office documents containing macros that run the subsequent stage of the malware or using hijacked email threads with .zip attachments. IcedID surged in March and April 2021, with new tactics and increased spam volume, leading many to believe it is the current successor to Emotet.

Unlike other botnets, IcedID does not openly track any of its clients or users, although we believe its developers operate an affiliate model. IcedID is also less mature in its infrastructure operational security, continuing to use the same pool of servers for its operations. Although this is effective in generating infections, it does not display the same maturity as the other families mentioned.

Financially Motivated Cybercrime

Cybercriminals have continued to demonstrate flexibility and ingenuity in using botnet operations. Recorded Future analyzed threat actor dark web posts and publicly reported intelligence to gain insight into which nations and regions appear to be particularly targeted by threat actors advertising botnets as a service in various languages. During our investigation, Recorded Future found Portuguese, Spanish, Russian, English, and Chinese to be among some of the more popular languages for conversations about botnets being sold, created, and used to target victims.

Portuguese and Spanish

Although on January 27, 2021, a global team of law enforcement agencies announced the seizure and takedown of Emotet, during its life the majority of Emotet controllers resolved to IP addresses in Latin American countries. The threat actors behind the infamous botnet (which has evolved from its beginnings as a banking trojan into a full-service threat delivery service) were surging in the region, targeting an array of sectors, from automotive to finance and retail to technology. While there are other botnets leveraged in the region, Emotet was heavily favored in comparison to other botnets prior to its takedown among Portuguese and Spanish-speaking threat actors.

Since its dismantling, Recorded Future analysts have seen cybercriminals in Latin America take to underground forums and marketplaces to advertise and sell their self-created as well as popularly known botnets. Below is a sample of events pertaining to botnets that have occurred within the past year on Spanish and Portuguese-speaking threat actors across the criminal underground:

Source	Intelligence
Cracked	The Portuguese-speaking threat actor "Pleek" posted an advertisement for botnet tutorials amongst other tools in September 2020 as a hacking package.
Cracked	The Portuguese-speaking threat actor "skandalozem" shared in March 2020 a botnet that they claim can perform distributed-denial-of-service (DDoS) attacks on any server.
Boveda Forum	The Spanish-speaking threat actor "therealghostcard" advertised their services and product for what they claim to be a 100% functional and stable botnet for android which includes 24/7 assistance, administration, injections, SMS interceptors, and hidden SMS interceptors.
Boveda Forum	The Spanish-speaking threat actor "Design3rK" requested business partnerships and associates to set up a botnet to generate scams in Spain.
Cebolla Chan Forums	The Spanish-speaking threat actor "leet331" shared a post in which they sought botnet partners to collaborate and administer a homemade botnet which includes modules such as keylogging, screenshot module, and cookie stealer module.

Table 1: Breakdown of Spanish- and Portuguese-speaking threat actors (Source: Recorded Future)

Chinese

APT use of botnets

On July 21, 2021, the Record reported that China's APT31 has been hijacking home routers to form a proxy botnet around its server infrastructure to relay and disguise its origins. A security alert published by the French National Cybersecurity Agency, also known as ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), listed 161 IP addresses hijacked by APT31 in recent attacks against French organizations. French officials said that APT31's proxy botnet was used to perform both reconnaissance operations against their targets, but also to carry out the attacks themselves.

Cybercriminal use of botnets

On September 1, 2021, the Record reported that Chinese authorities had arrested the authors of the Mozi Internet of Things (IoT) botnet. At its peak, the Mozi botnet infected 160,000 systems/day in September 2020 and had historically infected more than 1.5 million different devices, with more than half of them located inside China. The botnet also used the DHT protocol to create a P2P system between all the infected devices, allowing bots to send updates and operational instructions to each other directly, which also permitted Mozi to continue to operate even without a central C2 server. For this reason, researchers believe it will take months for the botnet to die out. In addition, prior to their arrests, new features were added to the Mozi module which enabled cryptocurrency mining on infected systems in an attempt to monetize the botnet beyond DDoS attacks.

Scripts and tutorials for cryptocurrency mining that uses a botnet are widely offered on Chinese-language dark web marketplaces. On June 3, 2021, the threat actor "wo98998998" advertised an offer for the script and tutorial for utilizing a botnet for cryptocurrency mining on Dark Web Exchange. A similar offer was posted by the threat actor "456811" on Tea Horse Road Market on June 4, 2021.

Botnet capability is often packaged with other hacking tools and offered for purchase across the Chinese-language dark web ecosystem. On June 11, 2021, the threat actor "409272" offered a toolkit dubbed the "Hack Pack" on Tea Horse Road Market that included anti-antivirus, password cracker, DDoS, vulnerability scanner, and other functions. A similar offer was posted by the threat actor "665317" on Exchange Market on June 17, 2021.

In a telegram post on August 7, 2021, the threat actor "aihacker" stated the sale of the botnet for DDoS started on July 25, 2021, with UDP at 1 T, ACK at 500 G, large packet SYN at 260 G, and small packet SYN at 140 G. Customers have the option to purchase daily, weekly, and monthly DDoS service packages.

In addition to dark web marketplaces and Telegram, advertisements of botnet/DDoS services can often be found on Chinese-language clearnet hacking forums. Below are 2 advertisement banners from 16hk[.]com. The top one is for "云溪 (Cloud Creek) Specialized DDoS Service", whose operator claims to have been in operation for 3 years and takes orders for DDoS and CC stress testing services. It also lists the QQ number of 156740798 as a contact. The bottom one is for "孙悟空 (Sun Wukong, or Monkey King) DDoS Service", whose operator provides L4/L7 DDoS attacks.

Figure 2: Botnet/DDoS service ad banners on the Chinese-language hacking forum 16hk[.]com (Source: Recorded Future)

In addition, we observed possible Chinese-speaking threat actors offering botnets on Russian and English-language forums. The threat actor "everlongddos" advertised a 700 GBPS UDP botnet in both Chinese and Russian on the mid-tier Russian language forum Best Hack Forum, with everlongddos offering to perform demonstrations for serious customers. There is an instance of Chinese-language usage that hinted the threat actor might not be a native speaker, but the posting was clearly aimed toward Chinese-speaking forum users.

English

Overall, cybercriminals have continued to demonstrate the flexibility and dynamic aspect of a botnet operation by exploiting routers and other similar devices to perform unconventional tasks. Vulnerable IoT devices will likely remain instrumental in botnet operations, assisting with malware propagation efforts and attempts by threat actors to disrupt the networks for financial or political gain. Cybercriminal stresser/booter services are often sold as Software-as-a-Service (SaaS), with tutorials and user support offered. These services provide the user with the software to direct an attack, including control of DDoS method(s). These stresser services generally incorporate botnets consisting of compromised hosts into the attack service. These services can often cost as little as $10 an hour. Additionally, IP stresser services usually hide the identity of the actual attacker using proxy servers and botnets for an attack, or by spoofing the traffic source in a reflective attack.

General open-source searches for "stresser" and "booter" services typically result in dozens of listings including some that advertise DDoS services along with botnets and servers for hire. The accessibility of these services (regardless of the degree of their sophistication) is likely to continue to be appealing for fledgling cybercriminal entities attempting to learn how to efficiently use a botnet in support of financially motivated criminal activity.

Recorded Future analysts have continued to observe a general shift among cybercriminal and financially motivated threat actors to disrupt business operations, often incorporating DDoS attacks as a secondary tactic or technique to support other threat activities such as the deployment of ransomware onto targets. "UNKN" (alias "Unknown"), an operator of ransomware, historically stated that they like the idea of the SunCrypt ransomware group encrypting the files, threatening to expose the data, and would also launch a massive DDoS attack against the infrastructure of a victim. In October 2020, UNKN had admitted that REvil was expanding on this concept, one that was incorporated by multiple ransomware groups throughout 2021 in a trend reminiscent of the rise of extortion websites. Additions such as this continue to demonstrate ransomware operators' willingness to incorporate features originally adopted by other ransomware crews so long as they have some degree of success in generating additional profit.

Despite takedown efforts from law enforcement entities worldwide, we continue to observe threat actors on underground forums and clearnet sources advertising a variety of DDoS services or tools on a regular basis. Many IoT botnets found on underground forums, and typically sold as separate services, are either based on source code from the Mirai botnet or other similar malware. As noted by TrendMicro, low-cost rentals mean that this type of botnet is readily available to all levels of cybercriminals, even those that may not have the skills to build and run their own botnets. We also noticed that some of these Mirai botnet rentals come with guarantees of protection against disruption of botnet hosting as part of the service. The predominant model for earning revenue with these botnets is still DDoS. However, we do expect cybercriminals to innovate more over time.

Vulnerabilities, when unpatched or ineffectively mitigated, can expose IoT devices on the network to outside attacks, such as use in botnets, network infiltration, data exposure/exfiltration, device takeover, and potentially compromise other devices, including non-IoT devices on the network. Additionally, some vulnerabilities in IoT devices can remain invisible and unpatched for some time due to their use in proprietary settings leaving the devices at a high risk of compromise by threat actors.

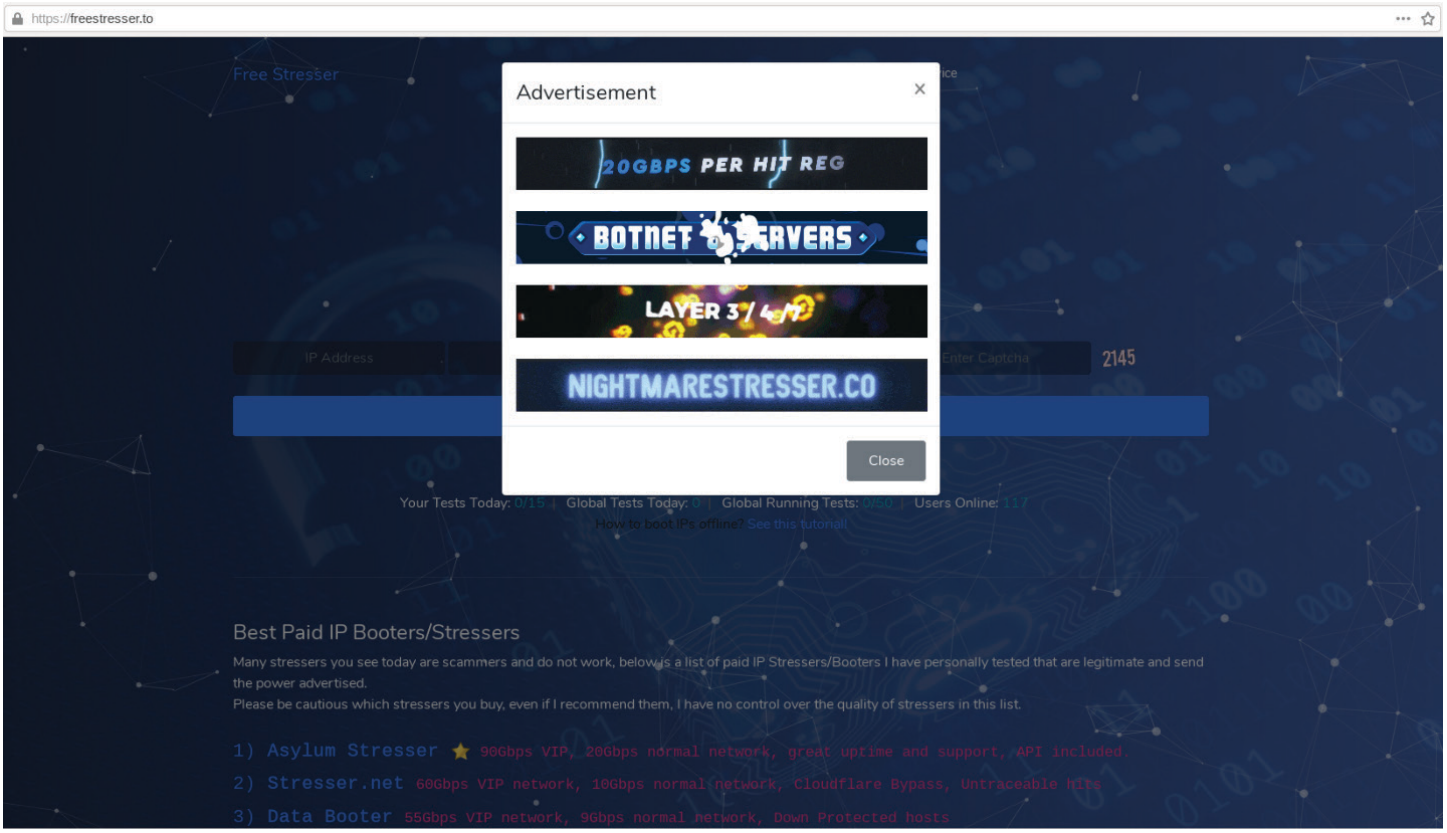


Figure 3: Advertisement for "stressers along with botnets" available for hire (Source: freestresser[.]to)

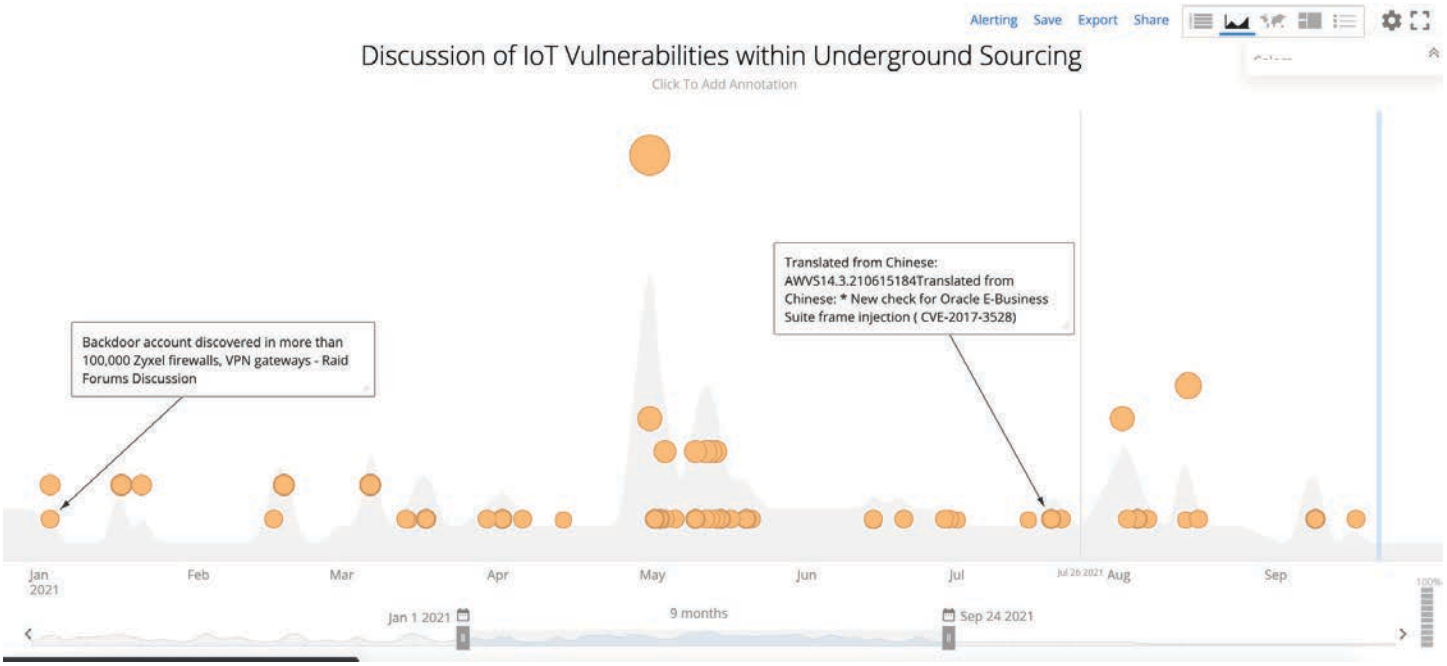


Figure 4: Discussions regarding IoT technology vulnerabilities within underground source reporting (Source: Recorded Future)

Several of the top threats associated with IoT devices that continue to be referenced within underground discussions include:

- Exploitation by IoT botnet malware (and being targeted by said botnets)
- Targeting/disruption of network infrastructure associated with legitimate businesses
- Brand damage through theft (or destruction) of employee personal or company data targeted by botnets distributing malware strains such as ransomware

The use of IoT technology on a network can greatly reduce operational costs, mitigate system issues, and improve across-the-board efficiencies. However, this innovation comes with unique security risks often resulting from attempts to combine this technology with legacy systems already functioning within a host environment. Among these risks to IoT systems include:

- A lack of uniform security standards in the maintenance of this technology
- Their utilization by building or facility managers rather than security professionals
- Their diverse irregularly secured attack surface allows threat actors potential access to company servers storing personal, proprietary, or financial data.

As society continues to place a large emphasis on making technology more efficient, both from a customer standpoint and an operational perspective, there continue to be security risks as modern technology is leveraged for convenience purposes rather than focusing on the end-to-end security of technologies they are utilizing.

Botnets Training: Inside the Bot-Herders School

In addition to the above botnet activities, Insikt Group analysts have identified dark web threat actors offering botnet-related services, including tutorials and lessons on how to use botnets in targeting victims. Since 2019, the Russian-language underground forum OpenCard has been offering a training course on botnets and bot-herders. OpenCard forum operates as a marketplace and discussion board focused on carding, e-commerce fraud, and money laundering. According to the course authors, "bot-herders are operators of botnets who use malware to break into computers and computer networks to form a botnet for personal gain and malicious purposes".

The price of entry into the Botnets and Bot-Herders School in September 2021 was $1,400. The courses are taught by 5 to 10 instructors — cybercriminals with a reputation in financial fraud, and OpenCard forum administrators and moderators. According to the OpenCard forum administrators, among the school instructors is a large botnet owner and a professor of a leading Russian university, and a chairperson of its IT faculty.

The average group of the Botnets and Bot-Herders School consists of 40 to 50 individuals with different levels of cybercrime experience, with most being novice fraudsters looking to build, maintain, and monetize botnets.

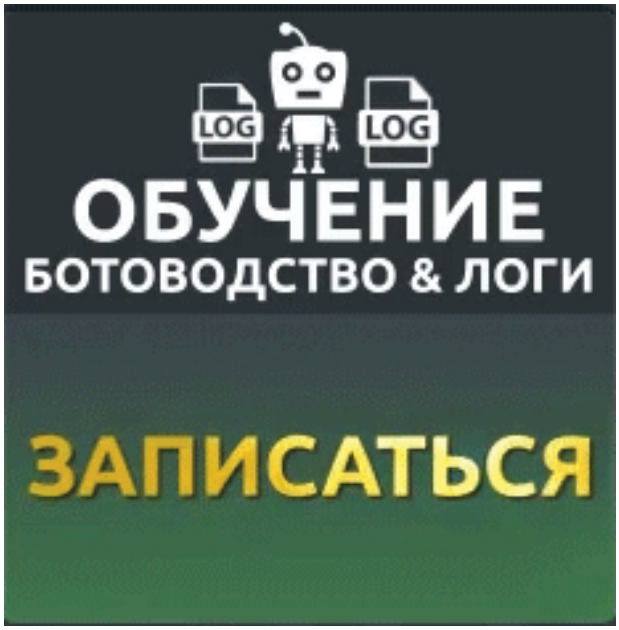


Figure 5: Botnets and Bot-Herders School. The description reads: "Training. Bot-herding & Logs. Sign Up" (Source: OpenCard Forum)

The Botnets and Bot-Herders School curriculum consists of the following training sessions:

1. Vulnerabilities of corporate networks
2. Examples of attacks on corporate IT infrastructure
3. Malware types and distribution methods
4. Installs: buying and making your own malware
5. Botnets: general concepts, classification, and monetization
6. Preparing, testing, and launching a botnet
7. Practical use cases with examples of successful botnet operations
8. Botnet security: avoiding closure and law enforcement attention
9. Web injects and exploits
10. Overview of the current botnet-related market
11. Logs: buying, mining, processing, and monetization methods

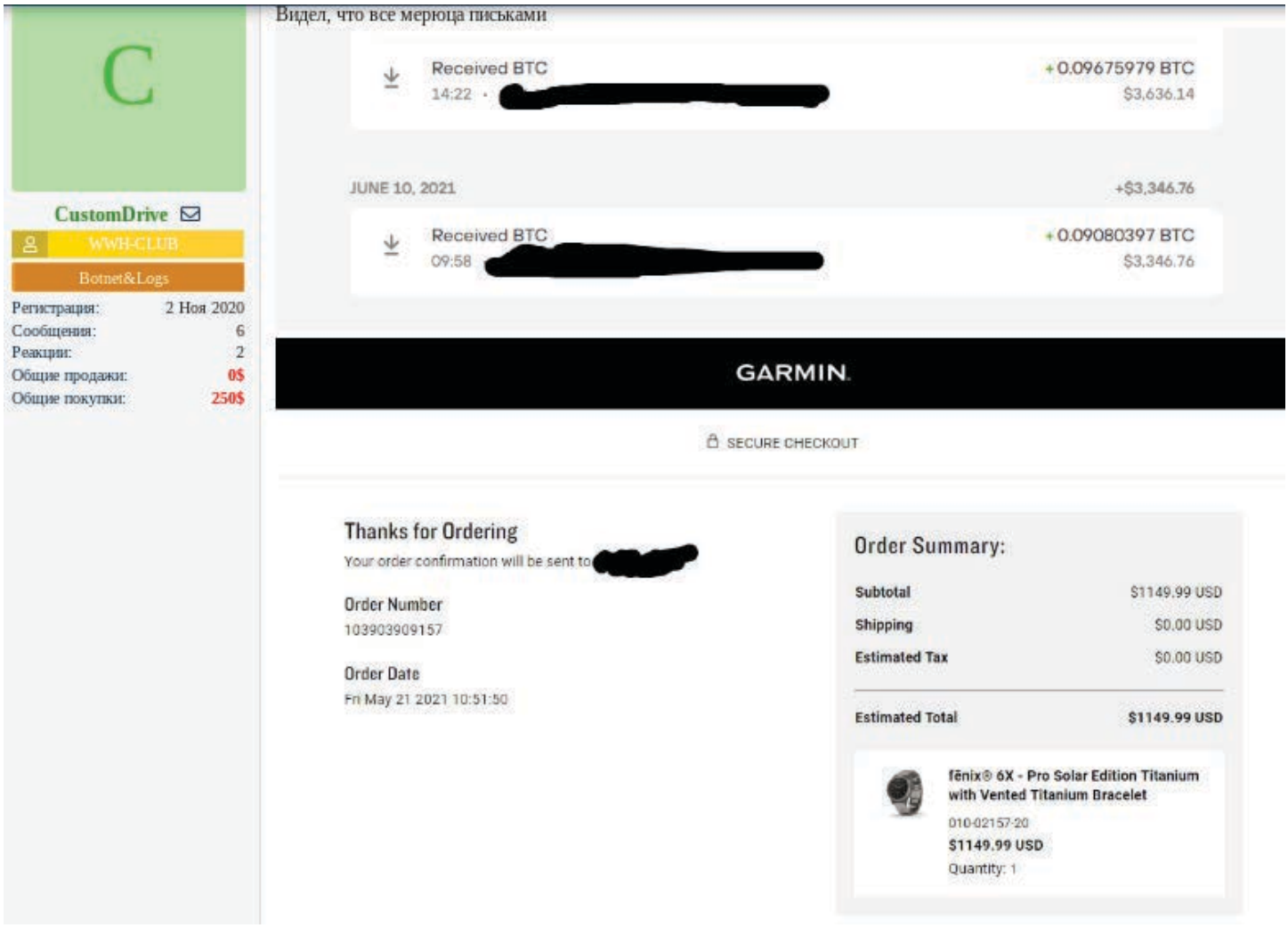


Figure 6: "CustomDrive", a graduate of the Botnets and Bot-Herders School, brags about stolen cryptocurrency and illegally purchased items using PII and login credentials obtained from infected users' computers (Source: WWH Club Forum)

OpenCard forum offers the Botnets and Bot-Herders School graduates a platform to find partners, and acquire the necessary components for launching and monetizing botnets.

The Botnets and Bot-Herders School instructors suggest using botnets for:

- Stealing PII, financial, and confidential information
- Launching DDoS attacks
- Creating SOCKS v4/v5 proxy servers, for example, for mimicking real users, sending spam, and facilitating payment card and other fraud
- Keylogging to record PII and confidential data, such as victims' logins and passwords
- Brute-forcing to use multiple infected machines and their computational power for password cracking
- Click-bots for monetization on the advertisement, such as auto-clicks on supplied URL links
- Adware for showing a contextual advertisement to infected users, rerouting victims' internet browsing to advertisements, and collecting marketing data on infected users
- Cryptocurrency mining, which according to the training instructors, is less profitable than other above-mentioned attack vectors

A botnet with 5,000 to 10,000 infected computers, according to the training instructors, can earn its operator up to $10,000 a day. At the same time, training instructors note that running a botnet is an expensive, risky, and not necessarily stable business. Yet, the Botnets and Bot-Herders School is well known in underground communities for enabling novice cybercriminals to enter the fraud stage. The Botnets and Bot-Herders School provides instructions on how to build and monetize a botnet and many graduates choose to use acquired skills for financial and credit card-related fraud, with some of the graduates using login and PII data they initially gain from infected computers for carding and shipment fraud.

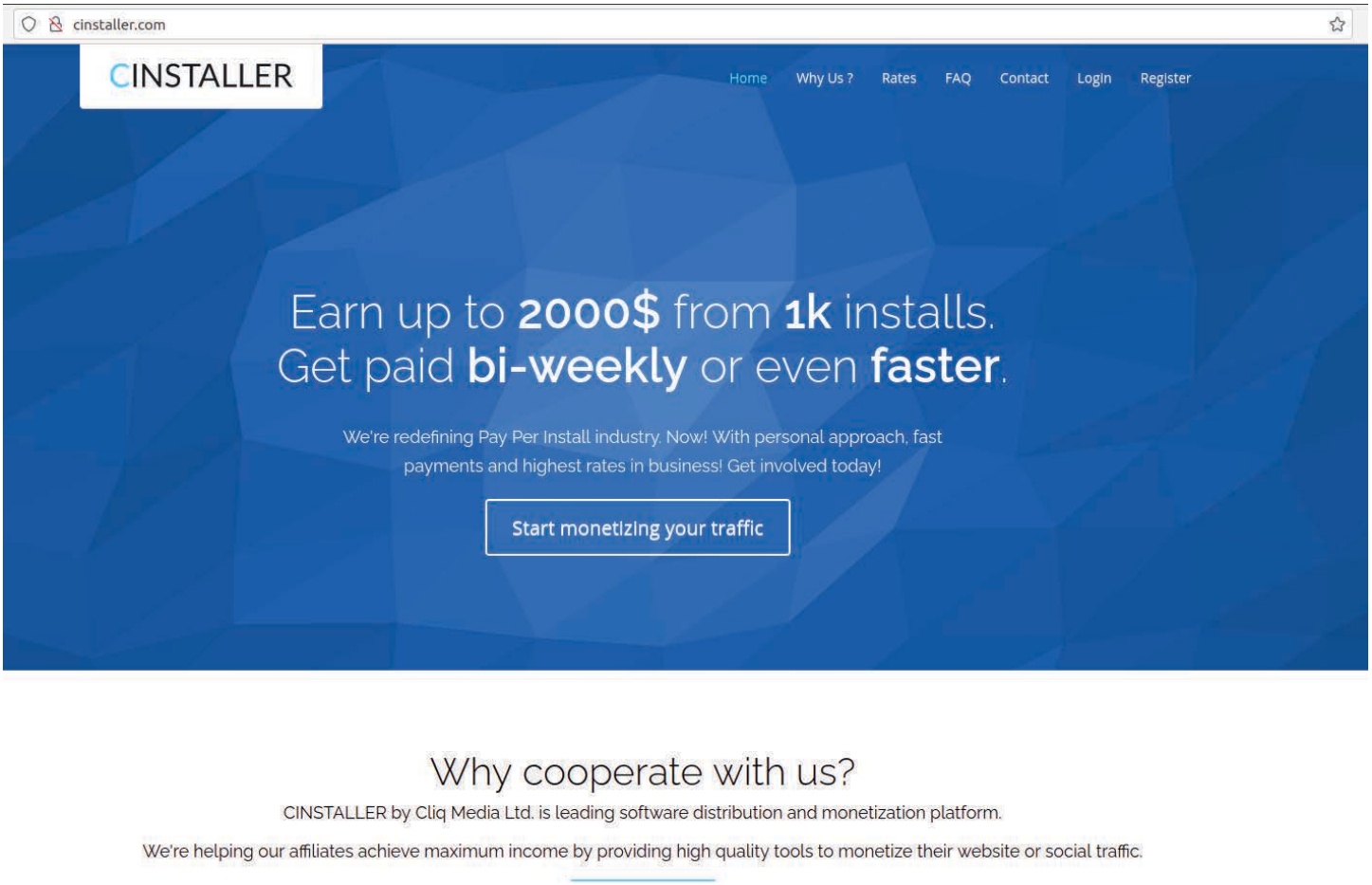


Figure 7: "cinstaller" website offering a platform to earn money from installs and web traffic (Source: cinstaller[.]com)

Using labor/freelance exchanges is a popular method for threat actors to infect multiple computers to form a botnet. Some labor/freelance exchanges allow the advertisement of software on their websites. Threat actors use this as means to advertise paid testing of software that is presented as legitimate products whereas it is packed with malware. Users who download and install this software, infect their computers that are turned into bots in a few clicks.

The malware is hidden inside the downloaded files that are usually not larger than 30 MB and appears as useful software, such as patches, utilities to enhance computer productivity, fitness applications, programs for accounting, management, IT, and many others. A cruel joke is for the threat actors to advertise malware-infused software as "cleaners, optimizers, or repair programs". Bots or infected machines are sometimes referred to as "installs" across the criminal underground. The most sought-after installs are from the US and the price varies between $500 to $800 per 1,000 installs. When infecting targeted computers, threat actors use loaders and crypters to elude anti-virus detections. The method of using labor exchanges in this fashion is very common but not considered among threat actors as the best for adding quality bots to a botnet. Threat actors pay as little as $1 per 1 installed piece of allegedly useful program that victims believe they test by downloading and installing while getting paid for a seemingly easy task. Some of the websites used for this method recommended by the Botnets and Bot-Herders School instructors are installunion[.]com, cinstaller[.]com, and installppi[.]com.

Lotteries and prizes are other popular methods threat actors use to infect multiple computers to form a botnet. For this method to work, threat actors can create a business page on a social network, such as Facebook, draw users to join the page, and make a post offering a lottery or a prize to those members who download and install software for testing and/or review purposes. This method requires many steps on the threat actor's part but is considered better for getting higher quality bots.

Another method widely employed by threat actors is to upload a malicious file, for example, listed as a new and popular computer game, onto a torrent-sharing service. According to threat actors, this method requires a significant amount of time

and maintenance to be successful but often brings high-quality bots, rich with PII and financial data ready to be pilfered. There are many other more and less targeted methods used by the threat actors to infect computers to form a botnet.

By the end of the Botnets and Bot-Herders School training, the new cohort of threat actors know how to find and distribute malware, infect computers, and form and monetize a botnet. Some of the trainees form smaller groups to join forces and share experiences of what works and does not work for them in bot-herding. Although the contents of the Botnets and Bot-Herders School may not always offer the latest tactics, since training instructors are likely to exploit novel methods before sharing them with the larger criminal underground audience, the materials and curriculum of Botnet and Bot-Herders School provide an insight into possible vulnerabilities as well as schemes and techniques used by threat actors.

Mitigations

There are several measures that organizations can implement to significantly reduce the risk of their Internet-enabled embedded devices from becoming targeted by roaming botnets. These security measures include:

- Ensuring that device firmware remains current and up to date at all times
- Integrating a virtual private network service
- Ensuring that the default manufacturer passwords are immediately changed upon acquiring a new device and that any existing devices within your enterprise that contain default credentials are immediately adjusted
- Ensuring that all ports unnecessary to the function of the device in question are closed

We proactively detect new botnet C2 servers to help clients prevent infections in their enterprises. We recommend automatically ingesting these servers for detection in firewall and IDS appliances and running them over SIEM logs to correlate infections. This includes proactive detections for all of the botnet families mentioned in this reporting.

We offer over 350 hunting packages that security teams can use to detect malicious activity based on malware signatures within their network. Due to the consistent shifting of packers used by the malware, we recommend using our SIGMA rules, which are available to clients, to detect the malware's behavior in place of static detection.

Further, we recommend the following mitigation strategies:

- Use the Recorded Future Platform to help identify actively exploited vulnerabilities and CVEs that have been positively associated with ransomware variants, which can help with patch management and prioritization.
- Keep systems and software up to date and have a reliable and tested backup method.
- Exposed Remote Desktop Protocol (RDP) servers are abused by threat actors to gain initial access into a target's network. If remote access solutions are crucial to daily operations, all remote access services (such as Citrix and RDP) should be implemented with two-factor or multi-factor authentication.
- Protect sensitive files using strong, complex passwords.

Outlook

The takedown attempt against TrickBot in the fall of 2020, and the successful takedown of Emotet in January 2021, have convinced botnet operators of the need to diversify. We expect botnet operators to continue to separate their operational infrastructure among affiliates to maintain their revenue streams. They will very likely continue to update their payloads with new packers, obfuscation techniques, and delivery tools, as they have always done, but they will likely apply those stealthy habits to their infrastructure as well. Continually evolving botnets will represent an ongoing threat to multiple industries due to their growing capability to not only disrupt, but to permanently render devices and services inoperable. Recorded Future has continued to see a growing level of technical sophistication among multiple threat groups, with entities backed by foreign governments demonstrating through their actions an interest in leveraging botnets to target critical infrastructure in both public and private sectors as well as SCADA/ICS devices.

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.