Recorded Future

CYBER THREAT ANALYSIS

Your Organization's Network Access Is King:

Here's What to Do About It

By Insikt Group®

CTA-2019-1030

Insikt Group used the Recorded Future® Platform to provide deeper insight into the monetization mechanisms for unauthorized access, and lay out extensive risk mitigation strategies for combating unauthorized access by using security intelligence. This report will be of interest to enterprises concerned with unauthorized access and corresponding methodologies for reducing risk.

Executive Summary

Historically, pay-per-install (PPI) services were the primary monetization route in the underground economy (UE) for commodity botnet operators. While botnets continue to feed PPI services, Recorded Future's data reveals that offerings of unauthorized access are increasing, driven by larger monetization opportunities via direct sales or auctions in underground forums.

Insikt Group assesses with medium confidence, based on Recorded Future analysis, that the demand in the UE for direct unauthorized access will continue to increase, leading to expanding opportunistic and targeted attacks. After observing sales and auctions on forums in the UE and communicating with threat actors, Insikt Group assesses that initial unauthorized access (sold in underground forums) is primarily accomplished with phishing, credential reuse, web shell placement, or exploitation of misconfigured or vulnerable software.

Key Judgments

- Advertisements for pay-per-install (PPI) services and direct sales of unauthorized access have increased over threefold in 2017, and continue to increase over time.
- Similarly, the number of unique monikers advertising PPI services and unauthorized access more than tripled in 2017, and has increased year over year.
- Judging by the annual increases in the sale of unauthorized access, criminal actors have concluded that they will maximize their profits through selling to other criminal actors, either through individual sales or auctions.
- Public sector and enterprise organizations will likely experience an increase in targeted and opportunistic attacks as more actors attempt to satiate demand for specific unauthorized network access.
- Information security practitioners must focus on preventing and detecting the four primary mechanisms for gaining initial unauthorized access: phishing, credential reuse, web shell placement, and exploiting known software vulnerabilities

Surveying the Underground Economy

The underground economy (UE) is made up of online actors who facilitate the buying and selling of criminal goods and services like stolen payment card data and malware. Pay-per-install (PPI) services and direct sales of unauthorized access are two growing parts of the UE that compromise organizational network security.

- PPI platforms are easy ways for buyers to quickly access lots of compromised computers to install malware payloads.
- Direct unauthorized access to specific types of networks is more profitable when sold or auctioned on the UE, but can take more time to obtain.

Unauthorized Access on the Rise

Ads for PPI malware services and direct sales of unauthorized access tripled in 2017 and continue to increase.

3X The number of advertisers for PPI services and unauthorized access increased more than 3X in 2017 and continues to rise.

Inside the Malware Marketplace

THERE ARE FOUR PRIMARY WAYS THREAT ACTORS GAIN INITIAL UNAUTHORIZED ACCESS:

PHISHING
Suspicious emails or instant messages from hackers pretending to be someone you know asking for personal information

CREDENTIAL REUSE
Usernames and passwords used repeatedly across multiple services that are easy to "stuff" into login portals across the web

WEB SHELLS
Malicious scripts uploaded to servers that provide remote access to file systems

SOFTWARE VULNERABILITIES
Specially targeted tools or techniques used to perform unauthorized actions by exploiting a system weakness

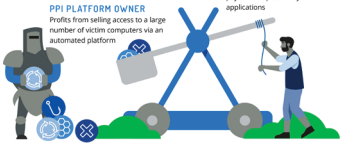
Knights of the Wrong Table

The PPI ecosystem relies on three key players who conspire together to gain unauthorized network access:

Provides malware payloads or potentially unwanted applications such as trojans, ransomware, adware, or spyware

BOTNET OR EK OWNER
Manages a network of hacked computers and distributes malware payloads or potentially unwanted applications

PPI PLATFORM OWNER
Profits from selling access to a large number of victim computers via an automated platform



PPI and Unauthorized Access

Number of authors by year mentioning either unauthorized access or PPI on criminal underground forums.

Preventing and Detecting Key Threats

En garde! Information security wizards must focus on preventing and detecting the four primary pathways for gaining initial unauthorized access.

PHISHING
Review quarantined email content and use security intelligence to identify new domains likely to be used for phishing

CREDENTIAL REUSE
Remove applications not using multi-factor authentication and surface compromised credentials from database breaches

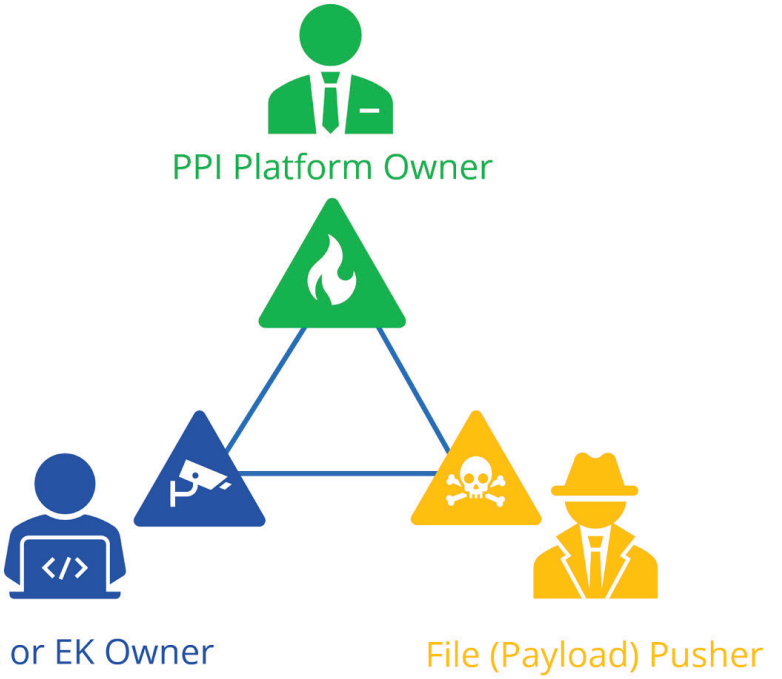
WEB SHELLS
Monitor web application firewalls and continuously identify new web shells with security intelligence

SOFTWARE VULNERABILITIES
Prioritize patching known vulnerabilities and look for evidence of "in-the-wild" exploitation

Learn more about securing your network
RECORDEDFUTURE.COM

Background

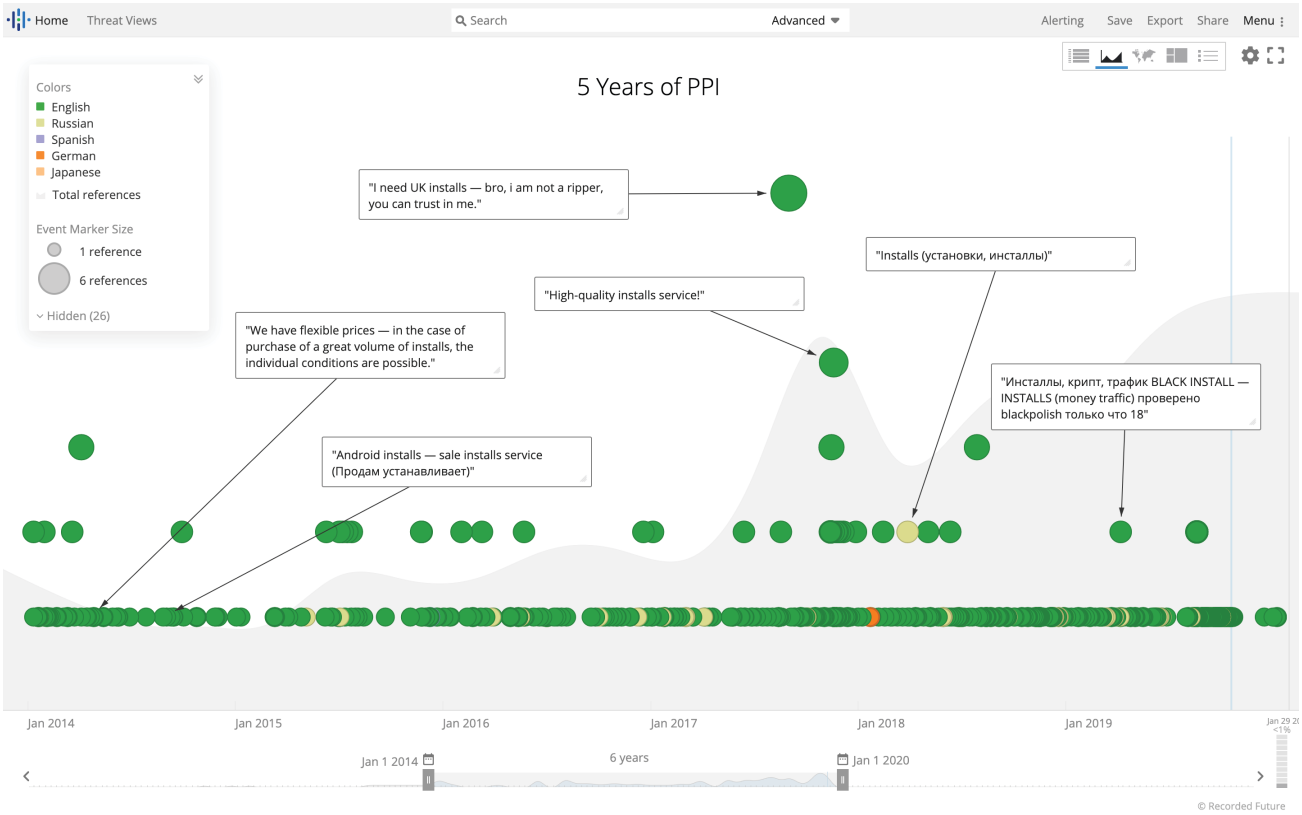
The underground economy (UE) is the totality of online actors and technology that facilitate the buying, selling, and trading of criminal goods and services. The UE has continually innovated and matured to maximize profits and avoid prosecution. Historically, much of the UE was focused on obtaining and monetizing stolen payment card data, but in 2007, the advent of multi-featured HTTP-based botnets like Zeus created a popular cottage industry known as pay-per-install (PPI).



The pay-per-install (PPI) ecosystem.

PPI relies on automated platforms where buyers pay for unauthorized access to victim computers to install malware payloads and/or other potentially unwanted applications (PUA). The price charged for each compromised computer is typically dependent on buyer demand for the country where the victim computers are located. PPI platforms (also known as affiliate networks) are natural third-party conduits for large infection (botnet or exploit kit) monetization. The PPI model is straightforward, but using a PPI platform introduces risk for botnet operators due to purposefully inaccurate installation statistics that increase profits for the PPI platform owner.

Similarly, PPI platforms are convenient mechanisms for buyers to quickly access large amounts of compromised computers and install further payloads, such as banking trojans, ransomware, adware, or spyware. The PPI model treats all infections/compromises as a generic commodity, regardless of victim organization — government, corporate, or residential. Traditionally, the only price differentiator is geography.

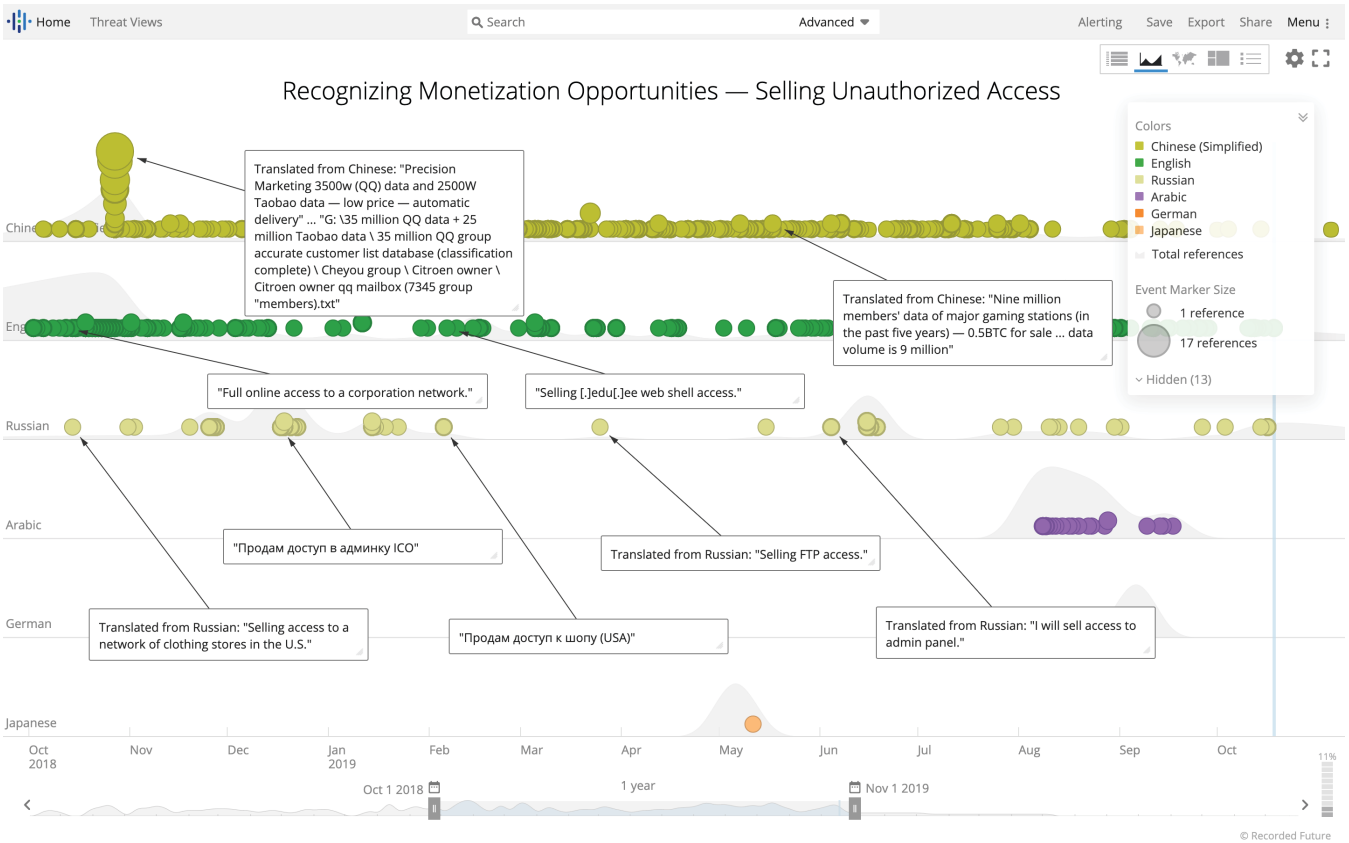


Advertisements of pay-per-install (PPI) services on the criminal underground.
(Source: Recorded Future)

Conversely, UE actors are recognizing that unauthorized access to specific types of systems may translate to increased monetization potential. Actors are directly selling (or auctioning) unauthorized access through UE forums, which may involve more time and patience, but is more profitable than commodity PPI services.

The differences in monetization potential are stark. An actor capable of installing malware on 1,000 devices can expect a PPI service to pay between $0.05 and $0.20 per infection (depending on the geographic locations of the infected hosts). Even at the top end of the range, daily PPI revenue is $200 ($6,000 per month). This model treats any infection as a generic commodity, regardless of where the infection occurs.

Conversely, directly selling or auctioning access to one system or network (often a name brand enterprise or government agency) maximizes revenue. For example, Fxmsp Group is a prolific seller of unauthorized access, often securing $20,000 for access to one organization.



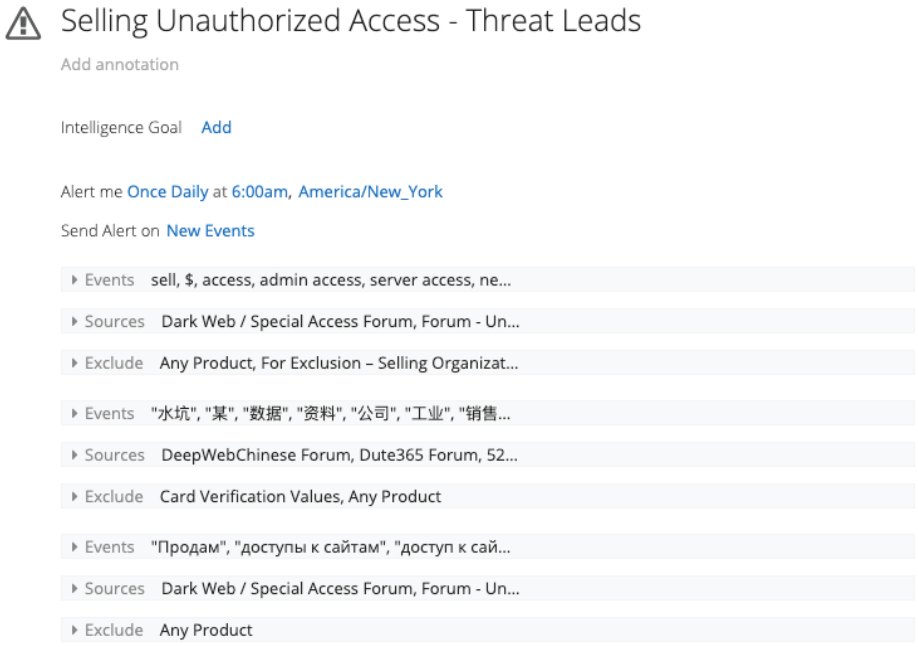
Selling specific network access at higher price points.
(Source: Recorded Future)

Threat Analysis

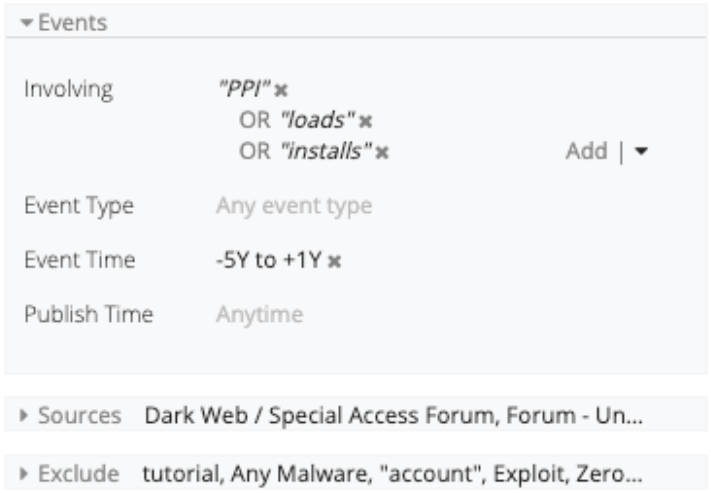
Increasing PPI and Unauthorized Access Advertising

Recorded Future's historical UE data demonstrates a year-over-year increase, beginning in 2016, in both PPI and unauthorized access advertising. The charts below illustrate the increasing advertising trends, which we expect to continue through 2019 (this year's data was measured in August). The metrics are consistent when measured by advertisement content, and also when measured by unique author moniker.

To collect data on underground forum references and authors, Insikt Group constructed queries for mentions of "PPI" and "unauthorized access" on the Recorded Future platform. The queries were conducted based on common entities surrounding sales of either PPI or unauthorized access into systems, as well as text matches for various sales terms in multiple languages. False positives were culled from the data set by altering existing queries. For example, sales language for "access to" card verification values were a common false positive in multiple queries. Thus, queries were altered to deliberately exclude those references.

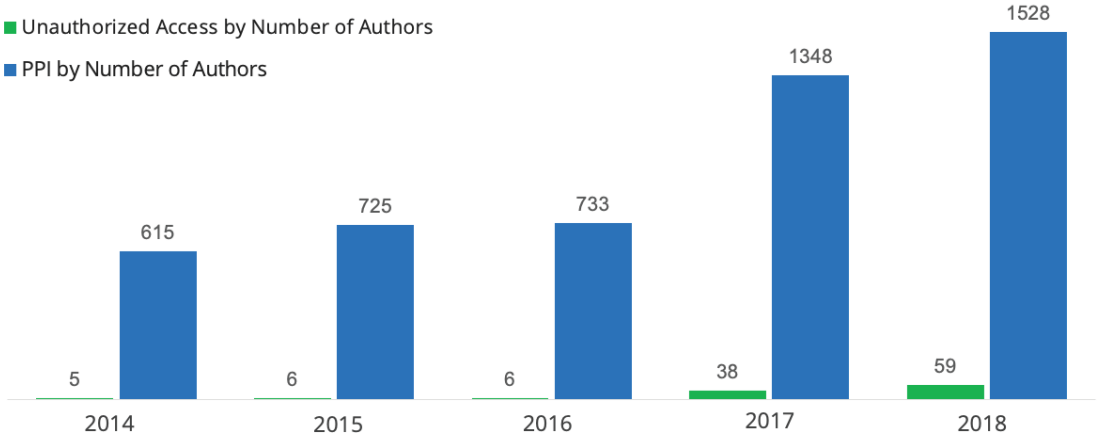


Unauthorized access query example.
(Source: Recorded Future)



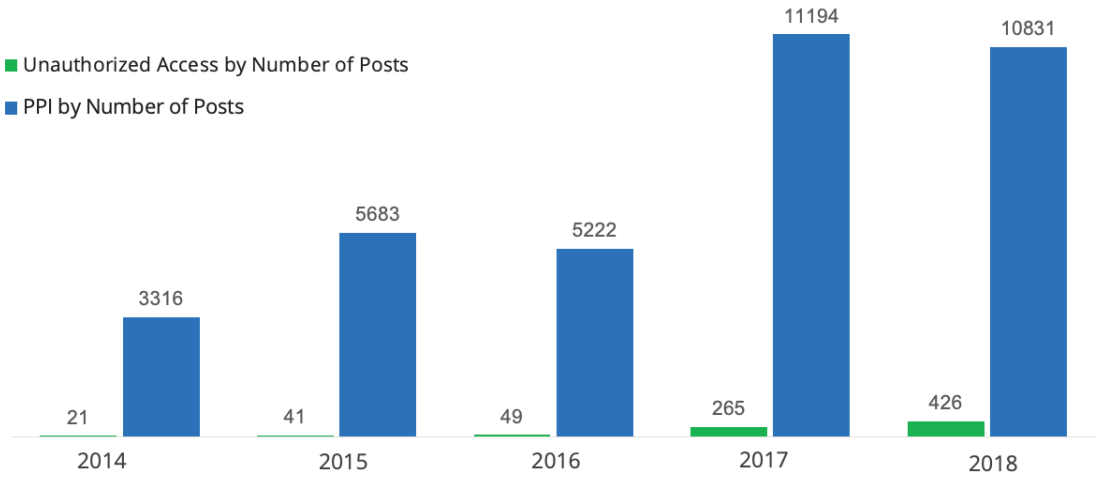
PPI English query example.
(Source: Recorded Future)

In addition, to count the number of actors mentioning either PPI or unauthorized access, while limiting as many false positives as possible, Insikt Group conducted automated aggregation of author monikers across multiple forums. Similar author monikers containing more than five letters (that were not common dictionary words) and posting on multiple forums only about PPI or unauthorized access were aggregated. While some of these monikers aggregated may not truly be the same actor, Insikt Group has assessed with medium confidence that a majority of these monikers are true positives, based on duplicate actor monikers and content. Furthermore, because the false duplicates are no longer counted, the data set represents a potential lower bound of the true number of PPI versus unauthorized access sales posts.



Number of authors by year mentioning either unauthorized access or PPI on criminal underground forums.

Based on the data, we were able to extract the number of authors mentioning unauthorized access and PPI in underground forums from January 2014 to September 2019. Unique monikers advertising PPI and unauthorized access have largely been increasing, and the number of authors from January to September 2019 is on par with the number of authors in previous years over a similar nine-month period.



Number of posts by year referencing either unauthorized access or PPI on criminal underground forums.

Similarly, Insikt Group gathered the posts pertaining to unauthorized access and PPI in underground forums from January 2014 to September 2019. The data also clearly shows that the number of PPI advertisements and unauthorized access advertisements has been steadily increasing.

Significant Global Access

Based on Recorded Future collection of unauthorized access advertised in forums, Insikt Group assesses with medium confidence that targeting is largely focused on the public sector and/or private sector enterprises, impacting organizations globally. Since Insikt's previous reporting on a Russian-speaking criminal selling unauthorized access to the U.S. Election Assistance Commission (EAC) in December 2016, Insikt Group has been regularly monitoring the sales of unauthorized access on the criminal underground. The following are a selection of notable sales or auctions based on the level of access being advertised and the potential for negative organizational impact. The access advertised by most actors are regularly vague and do not contain the specific names of victim organizations.

Analysis of the sales posts below, threat actor engagement, and analysis of unauthorized access auctions conducted by Insikt Group over the last four years, allows Insikt Group to assess with medium confidence that the following four attack vectors are — in no particular order of importance — the primary methods used to accomplish initial unauthorized access.

- Phishing
- Credential reuse
- Web shell placement
- Exploiting a known software vulnerability

Date	Actor	Access
December 2016	Rasputin	U.S. Election Assistance Commission (EAC)
October 2017	A_violent_god	A U.S. news website with two million readers
December 2017	Kindunkind	540 U.S. media company web shells and 15 admin panels of EU media resources ($22K)
May 2018	Maklaud	Moscow police traffic databases ($25K)
December 2018	Zifus	300 Italian e-commerce web shells ($3K)
January 2019	Tungsten	Asian e-commerce website ($10K)
March 2019	asadi64	Remote Desktop Protocol (RDP) access to a large U.S. oil company
March 2019	BigPetya (Fxmsp)	Asian automobile manufacturer
April 2019	vestl	VNC access to 22 computers across nine different U.S. hotels
April 2019	Aaaakkkka	Italian bank's internal loan computer ($2K)
May 2019	markopollo	Web shell access to a weapons factory
June 2019	truniger	RDP access with administrative privileges to an Italian municipality
June 2019	stilus	Customer relationship management (CRM) system of a New Zealand investment firm ($10K)

Date	Actor	Access
June 2019	AD0	Corporate network of an international online retailer ($25K)
June 2019	Aaaakkkka	Sells access to an unspecified power company's server ($600)
August 2019	SHERIFF	Administrator access to the database of a large Australian commercial construction company ($12K)
August 2019	B.Wanted	Domain administrator rights for a network containing 19,000 PCs across 20 Louisiana health clinics
August 2019	bc.monster	U.S. energy corporation's network
August 2019	johnsherlock, infoshell	SSH (secure shell) access to the network of a multinational healthcare company
August 2019	-TMT-	Administrative access to the network of a Brazilian hypermarket chain
August 2019	VincentVega	Large Chinese financial firm (5BTC)
September 2019	Katavasya	New Zealand firearms and ammunition accessories e-commerce site
September 2019	Antony Moricone, (Fxmsp)	Corporate network of a German decorative lighting company, including 10 domain controllers
September 2019	Juventus1	Administrative web panel of an Asian airline
September 2019	Gabrie1	Network (containing over one thousand computers) of a U.S. oil and gas exploration company ($24K)
September 2019	0x4C37	High-traffic antivirus website ($8K)

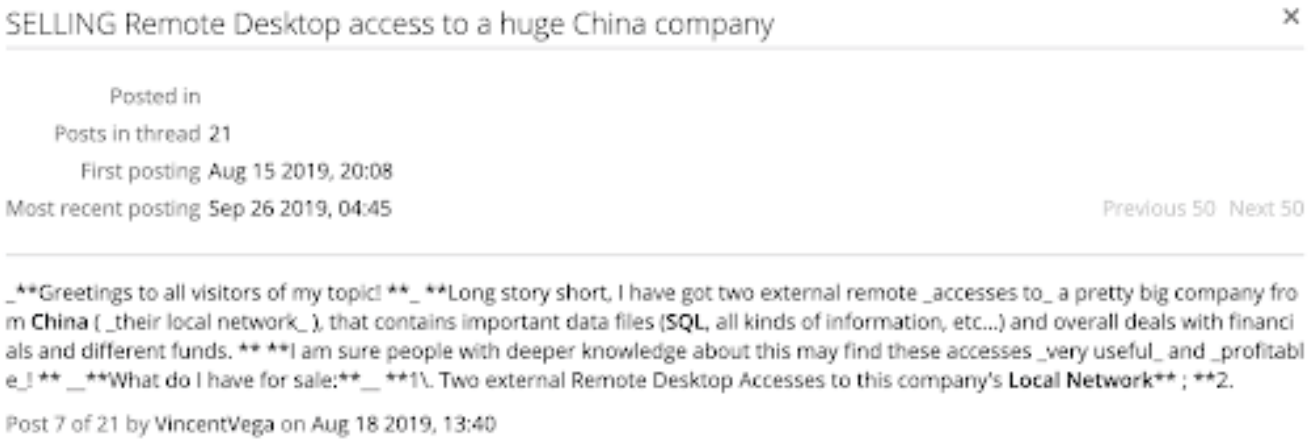
Selection of unauthorized access auctions and sales. (2016–2019)

Profiling 2 Unauthorized Access Sellers: VincentVega and Fxmsp

The two following case studies showcase the monetization potential of both targeted and opportunistic access.

VincentVega

VincentVega, a member of a high-profile, Russian-language criminal underground forum, is a prime example of an actor taking advantage of opportunistic access. The actor had gained access to one of China's largest investment banks and security companies (2015 reported revenue of 37.6 billion RMB) by brute-forcing RDP in an untargeted manner on internet-facing systems.



VincentVega advertising access to a Chinese company's internal network. (Source: Recorded Future)

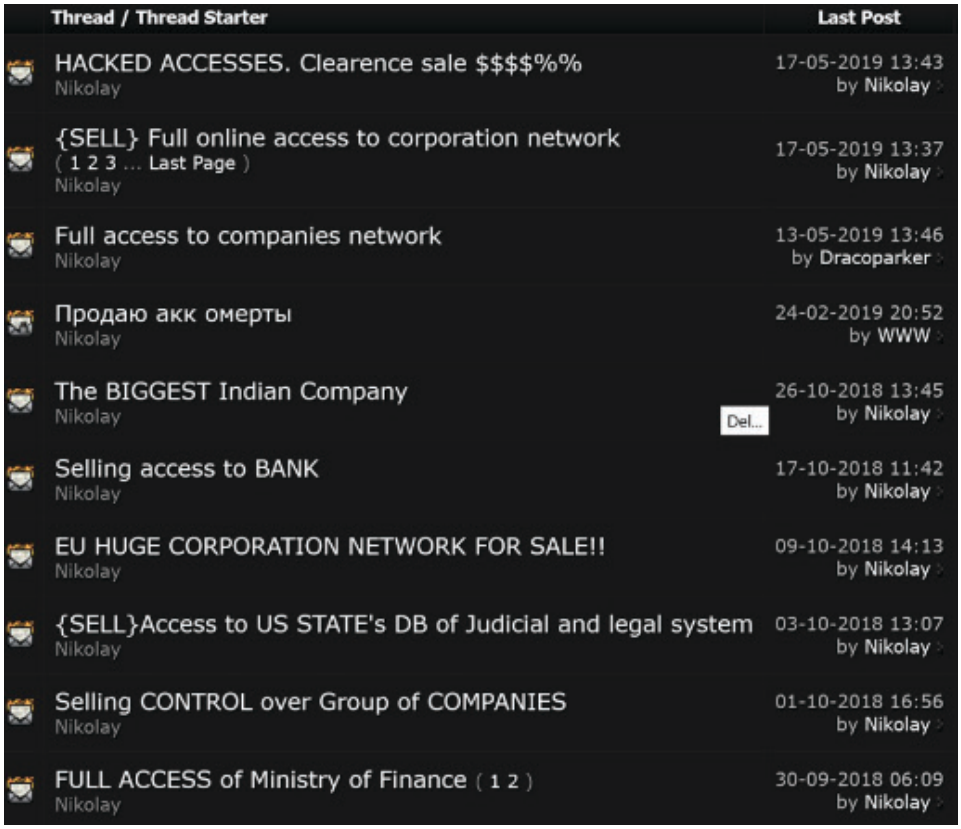
In August 2019, VincentVega advertised external remote access to a large Chinese company's local network for five Bitcoin. In their post, the actor claimed that they had initially accessed the network by brute-forcing IPs with RDP access. They claimed that the local network contains 20,000 working local IPs, approximately 865 of which have RDP access, while 500 of the victim hosts also have administrator access. In their post, they claimed to be selling the access because, while they understood that the access is valuable, they did not know how to monetize it.

Because of these admitted unknowns, Insikt Group assesses with high confidence that VincentVega, in an untargeted attempt to find IPs with poorly password-protected RDP services, stumbled upon

the company. However, once within the company's network itself, the actor realized that, based on the size and functionality of the network, there were multiple ways to monetize and sell access to the network itself.

Fxmsp Group

Fxmsp Group, on the other hand, clearly demonstrates how an organization can conduct unauthorized intrusions at scale to turn a hefty profit. The group is a Russian- and English-speaking cybercriminal collective that targets and sells unauthorized network access to a wide variety of global victims, including financial, e-commerce, industrial organizations, and governmental institutions. Fxmsp Group often compromises networks in bulk for the purpose of reselling to other cybercriminals. Since 2017, Fxmsp Group has compromised global corporate and government networks and subsequently sold the unauthorized access for amounts ranging from a few hundred dollars to over $100,000.



Posts by Nikolay of Fxmsp Group selling access to networks belonging to various organizations.

Fxmsp Group displays patience and coordination among team members. The actor using the moniker "Fxmsp" is charged with compromising networks, while the actors using the monikers "Lampeduza," "Antony Moricone," "Nikolay," "BigPetya," and others are responsible for maximizing unauthorized access monetization.

We assess with medium confidence that Fxmsp Group attempts to monetize unauthorized access through a network of private contacts before quasi-publicly creating a sales thread or auction for a larger pool of buyers. This suggests that forum auctions initiated by Fxmsp Group are only a fraction of the available unauthorized access that Fxmsp Group is attempting to monetize at any given time.

Outlook

We assess with high confidence that the volume of unauthorized access and direct sales with perceived victim value will continue to increase for the foreseeable future. Malware-specific PPI affiliate services will continue to provide criminal value within the UE, but malware infections are less profitable in the PPI system than opportunistic and targeted unauthorized access.

Information security professionals should be focused on implementing and reviewing preventative best practices in conjunction with internal proactive detection efforts around the following four primary methods of establishing initial unauthorized access: phishing, credential reuse, web shell placement, and vulnerability exploitation.

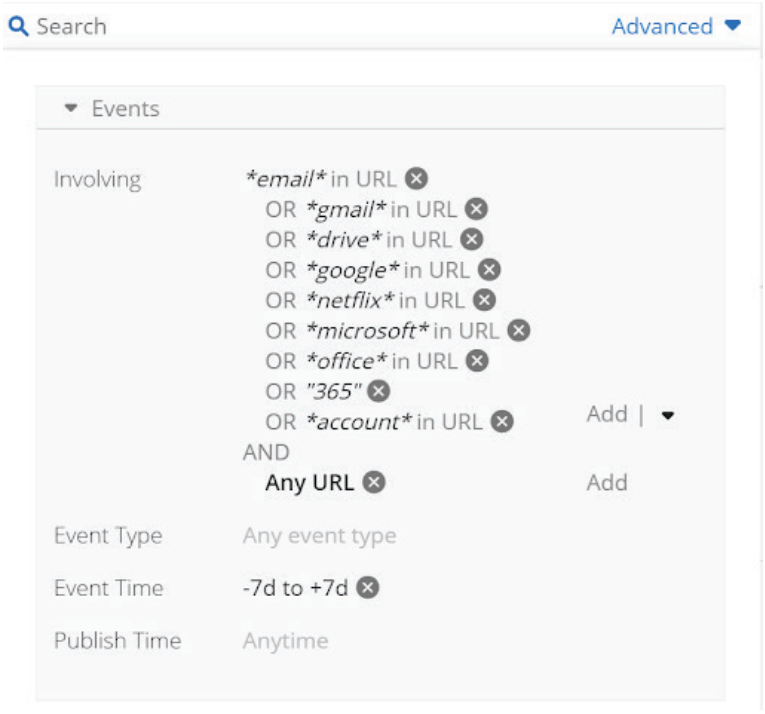
Risk Mitigation

Security intelligence is necessary to quickly detect initial unauthorized access via threat hunting methodologies. These methodologies should grow over time as operational practitioners increase their knowledge of adversary tactics and the internal network environment. A new methodology should lead to an ongoing hunting implementation via an automation/orchestration (SOAR) workflow. This section will provide mitigation recommendations for the four primary initial access methodologies found by Insikt Group.

Phishing

For example, reviewing email content and attachments quarantined by an email security gateway provides basic awareness of adversary tactics that have previously failed, while also presenting valuable examples where derivative technique modifications may succeed in the future. An email security appliance may be configured to block specific inbound file attachments[1] (for example, "hta" — HTML executable), but it fails to block malicious email containing third-party website links.

Thus, the focus of a phishing hunting methodology would in this case entail identifying new domains likely to be used for phishing (email body content) based on the domain's lexical proximity to prolific cloud provider domains (such as DocuSign, Google mail services, Microsoft Office365, Amazon storage, etc). Security intelligence provides new domain candidates which should then be used for improving email security gateway content inspection and detection in DNS telemetry or web proxy appliance resolution.



Recorded Future query to identify new phishing domains.

[1] https://www.cyber.gov.au/publications/malicious-email-mitigation-strategies

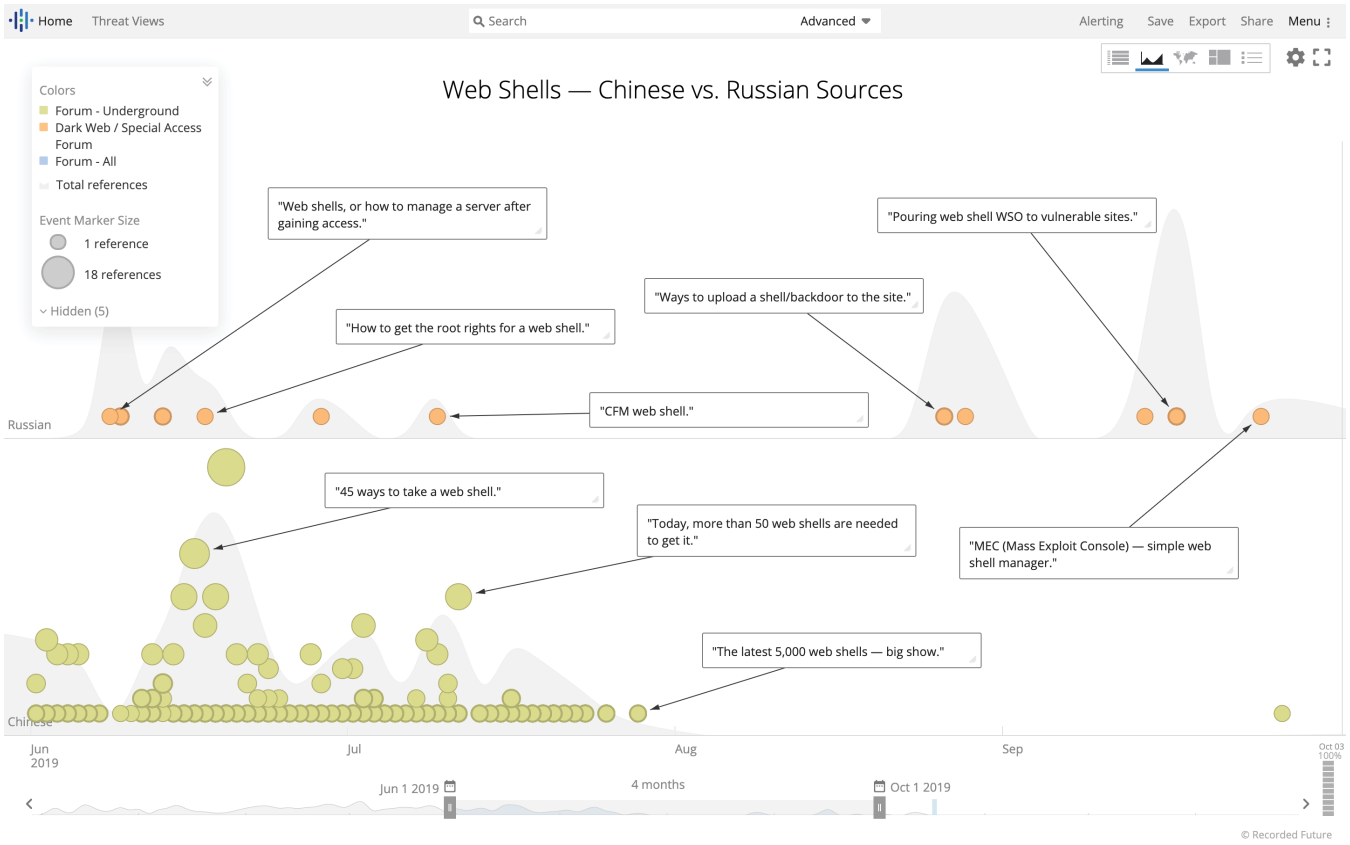
Credential Reuse

Vigilance in asset management and removing internet-facing systems running applications without multi-factor authentication is good hygiene for preventing credential reuse, and in the case of RDP, brute-force attacks. Security intelligence reduces the risk of adversary credential reuse by surfacing compromised credentials primarily from database breaches. The corresponding SOAR workflow should search Active Directory for users matching newly discovered credential sets. Whenever a valid user is found in a credential set, a password reset is initiated.

Web Shell Placement

Adversaries typically place web shells on web servers via a software vulnerability or misconfiguration. A web shell will often evade a web application firewall (WAF) and enable long-term persistence on one or more web servers. Adversaries use web shells to exploit information resources or gain unauthorized access to additional systems. Security intelligence is an important component of web shell hunting, which requires continuous identification of new web shells and associated feature assessments. For example, older web shells use basic, form, or digest HTTP authentication, which is straightforward to identify in network telemetry (Zeek is a valuable open source tool for network protocol parsing and analysis).

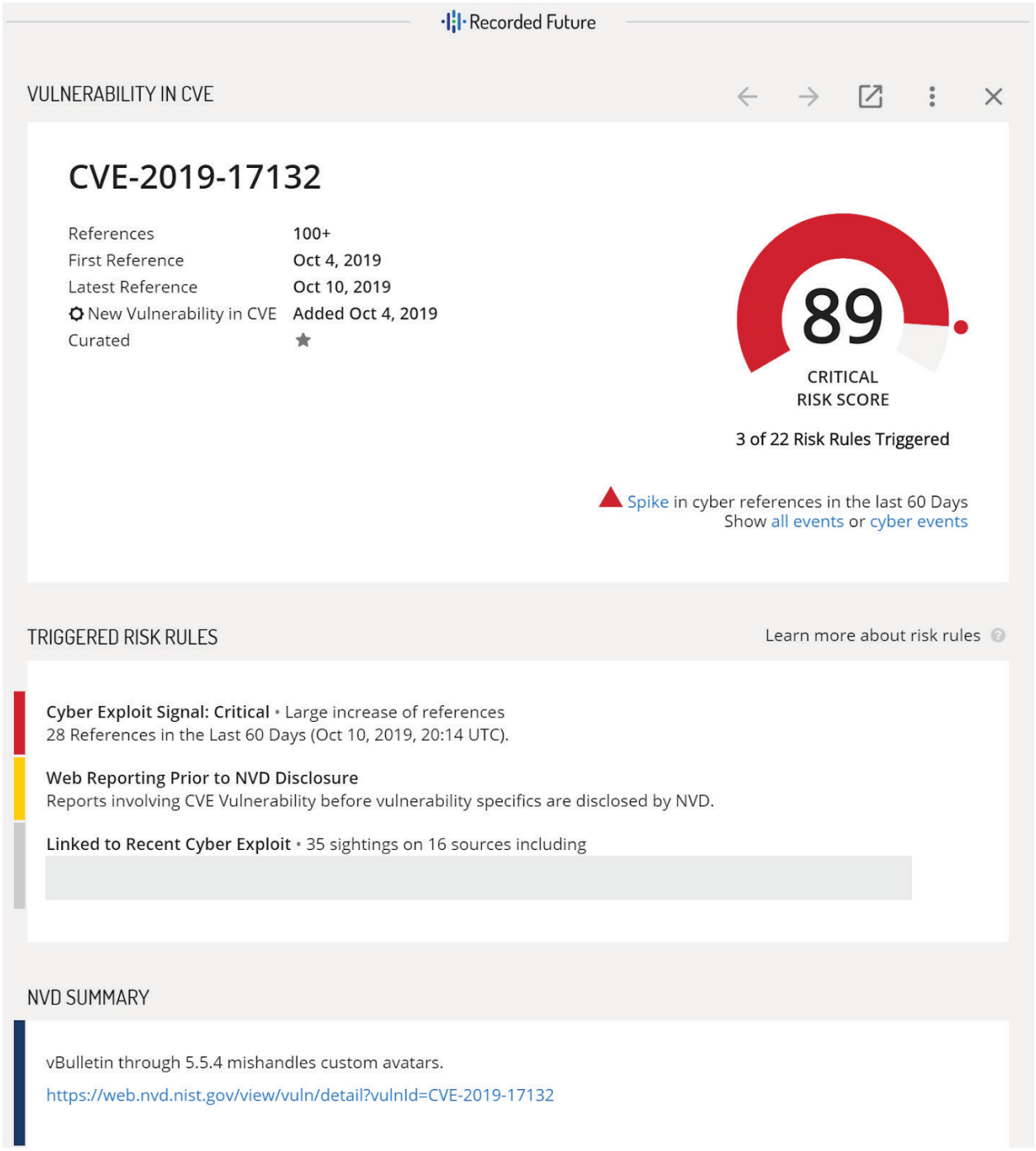
Additionally, YARA rules are another open source resource to identify specific web shells based on file conditions (typically strings).



Surfacing new web shells.
(Source: Recorded Future)

Exploiting a Known Software Vulnerability

Continuous patching prioritization and execution in an enterprise environment is challenging, but security intelligence can help by originating new pre-NVD vulnerabilities and enriching existing vulnerabilities, particularly with evidence of "in the wild" exploitation.



Additional vulnerability context provided by Recorded Future Intelligence Cards.
(Source: Recorded Future)

About Recorded Future

Recorded Future arms security teams with the only complete threat 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.