



# Pawn Storm in 2019

## A Year of Scanning and Credential Phishing on High-Profile Targets

Feike Hacquebord

## TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

Published by:

**Trend Micro Research**

Written by:

**Feike Hacquebord**

Stock image used under licensed from

Shutterstock.com

# Contents

**4**

Abusing High-Profile Email Addresses for Spam

**7**

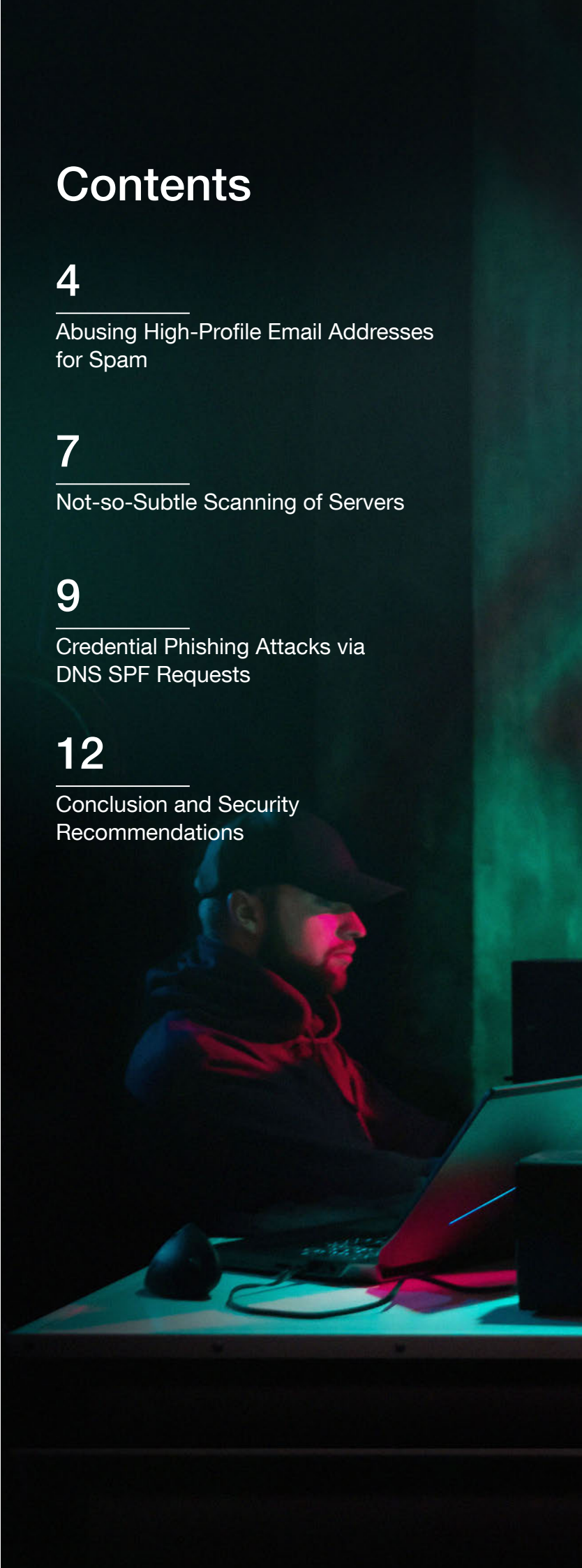
Not-so-Subtle Scanning of Servers

**9**


Credential Phishing Attacks via DNS SPF Requests

**12**

Conclusion and Security Recommendations







Pawn Storm has had traditional cyber weapons, like malware, in its attack arsenal since at least 2004,<sup>1</sup> the earliest year we have been able to trace the group's activities. Back in 2014<sup>2</sup> and 2017,<sup>3</sup> we wrote about the various attack vectors and methodologies of this advanced persistent threat (APT) group, which is also known as APT28, Strontium, and Fancy Bear. Over the years, we have unraveled how the group has employed spear-phishing emails, phishing sites, and malicious iframes, and how it targeted entities ranging from the defense industry and international organizations to media and political parties. Today, Pawn Storm continues to deploy malware against its targets, but it has also been seen directly attacking web and cloud services instead of taking the more common route of infecting targets through spear phishing.

Pawn Storm is a group that has shown ample resources and multifold strategies in its operations. The group has targeted many organizations, harvested considerable information, and attempted to influence mainstream media and public opinion. Due to Pawn Storm's notoriety, its attack methods have been well-documented. The threat actors behind Pawn Storm have used sophisticated social engineering lures, data-stealing malware, several zero-days, and even a private exploit kit.

This report aims to shed light on some of Pawn Storm's attacks that did not use malware in the initial stages. It presents new data on the group's credential phishing, direct probing of webmail and Microsoft Exchange Autodiscover servers, and large-scale scanning activities to search for vulnerable servers. Among the group's prominent targets were members of defense companies, embassies, governments, and the military. We will also disclose how we were able to track Pawn Storm's credential phishing campaigns over the past two years through careful analysis of DNS SPF requests of domain names used to name some of their computer server images.

# Abusing High-Profile Email Addresses for Spam

We have been closely following waves of the group’s targeted credential phishing attacks and have collected thousands of email samples that the Pawn Storm actors sent out since 2014. This data allowed us to see new trends in Pawn Storm’s tactics, techniques, and procedures (TTPs).

For instance, in May 2019, we observed something interesting: Pawn Storm started using hacked email addresses of numerous high-profile targets to send credential spam messages.

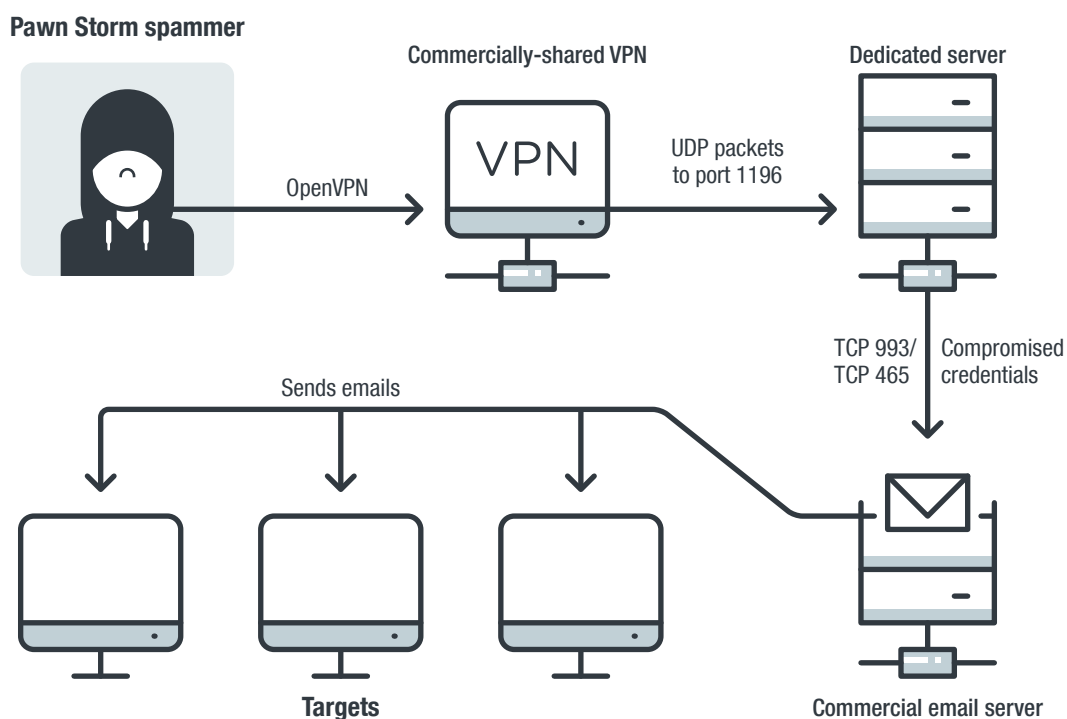


Figure 1. The setup Pawn Storm frequently used to send credential phishing spam in 2019

The actor connects to a dedicated server using the OpenVPN option of a commercial VPN provider and then uses compromised email credentials to send out credential spam via a commercial email service provider. The group used this scheme over an extended period in 2019 to 2020, with the most compromised email accounts belonging to defense companies in the Middle East.

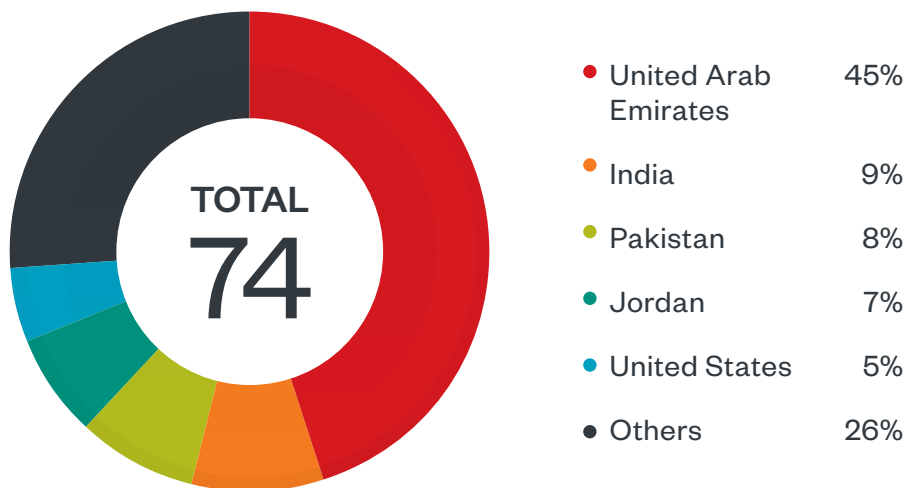


Figure 2. Breakdown of abused email servers for the period of May to December 2019, sorted by country

The reason for the shift to the use of compromised email accounts of (mostly) defense companies in the Middle East is unclear. Pawn Storm could be attempting to evade spam filtering at the cost of making some of their successful compromises known to security companies. However, we did not notice a significant change in successful inbox deliveries of the group's spam campaigns, making it difficult to understand the rationale behind the change in methodology.

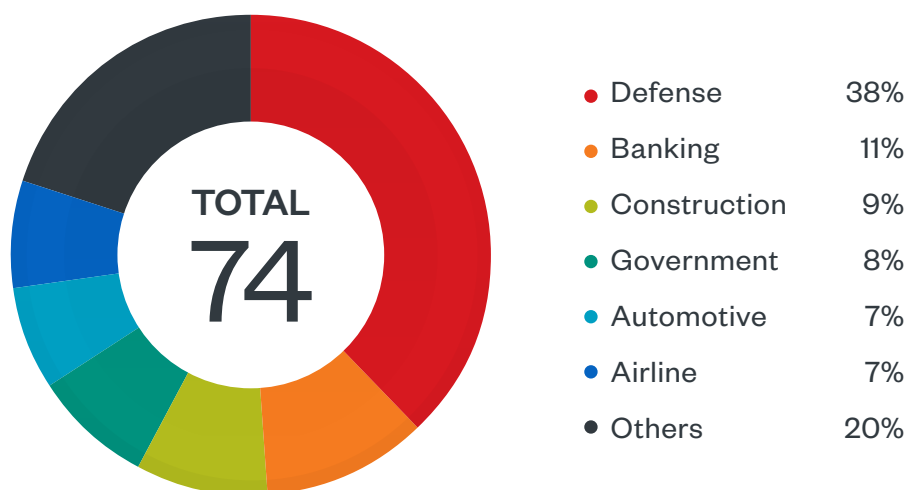


Figure 3. Breakdown of abused email addresses, sorted by industry for the period of May to December 2019

Figure 3 shows the breakdown of industries whose email addresses were abused to send out credential phishing spam. How Pawn Storm could be getting the email credentials of their targets is a point of interest. Malware could have been utilized to achieve this, but the group could also be using a method that involves brute-force attacks.

In 2019, Pawn Storm performed daily probes on numerous email servers and Microsoft Exchange Autodiscover servers across the world. The actor group was connecting to a variety of Transmission Control Protocol (TCP) ports that were related to email. We observed that most of the probing were aimed

at TCP port 443 (used by webmail and Microsoft Exchange Autodiscover services), while email protocols like the Internet Message Access Protocol (IMAP) [143, 993], the Post Office Protocol 3 (POP3) [110, 995], and the Simple Mail Transfer Protocol (SMTP) [465, 587] were also checked.

This was done in an apparent attempt to look for vulnerable systems, brute force credentials, exfiltrate email data, and send out spam waves. We have data on months of probing against hundreds of email servers worldwide and can thus make semi-statistical breakdowns by industry and by country or region. These breakdowns strongly depend on the different interests of Pawn Storm that vary over time.

Below we listed a sample of Pawn Storm’s typical targets from August 2019 to November 2019.

First Probe	Last Probe	Target	Region
8/2/19	8/2/19	Defense company	Southern Europe
8/5/19	8/5/19	Civil aviation authority	Africa
8/7/19	8/7/19	Airport	Africa
8/7/19	8/7/19	Government	Southern Europe
<b>8/15/19</b>	<b>8/21/19</b>	<b>Military</b>	<b>South America</b>
<b>8/16/19</b>	<b>8/22/19</b>	<b>Government</b>	<b>Middle East</b>
8/28/19	8/28/19	Law firm	Germany
8/29/19	8/29/19	Aeronautics company	Europe
9/2/19	9/2/19	Private school	France
9/2/19	9/6/19	Railway company	Eastern Europe
9/2/19	9/7/19	Oil and gas company	UK
9/2/19	9/8/19	Bank	US
9/3/19	9/9/19	Academic institution	South America
9/6/19	9/9/19	Multinational electronics company	Asia
9/7/19	9/7/19	Nutrition company	UK
9/8/19	9/8/19	Political party	The Nordics
10/3/19	10/3/19	Group of surgeons	Australia
10/3/19	10/3/19	IT company	France
10/3/19	10/3/19	Private school	UK
10/4/19	10/4/19	IT company	Netherlands

Table 1. The nature of organizations that had their email server scanned by Pawn Storm (mail, Autodiscover on port 443 and/or IMAP on port 993)

For the entries in red, we suspect Pawn Storm performed large-scale data exfiltration, based on the significant amount of data that was transferred in those timeframes and the duration of the connections made.

We found some of the group’s typical targets in the list, such as armed forces, defense companies, governments, law firms, political parties, and universities. Surprisingly, the list also included a couple of private schools in France and the United Kingdom, and even a kindergarten in Germany.

## Not-so-Subtle Scanning of Servers

Pawn Storm appeared to do large-scale scans on TCP ports 445 and 1433 as well, but in a way that wasn't subtle. The same IP address that has been hosting some of Pawn Storm's websites (for phishing free webmail credentials of high-profile users) has been scanning port 445 and port 1433 of computer servers across the world. This appears to be an attempt to find vulnerable servers running Microsoft SQL Server and Directory Services.

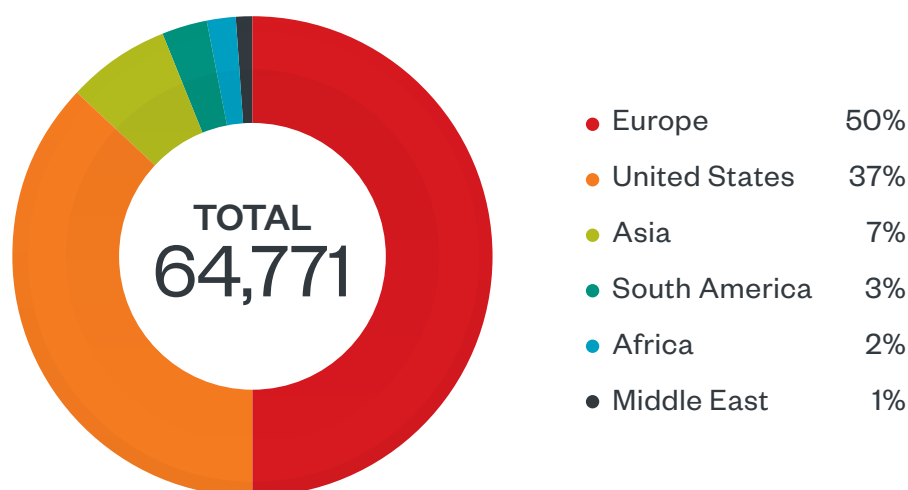


Figure 4. Breakdown of Pawn Storm's port scans on target IP address (via port 445), by country/region

The scans were done from the IP address 185.245.85[.]178 from November until December 2019. It should be noted that the exact statistics could differ in other time ranges because the targets of Pawn Storm's scanning depend on specific campaigns.

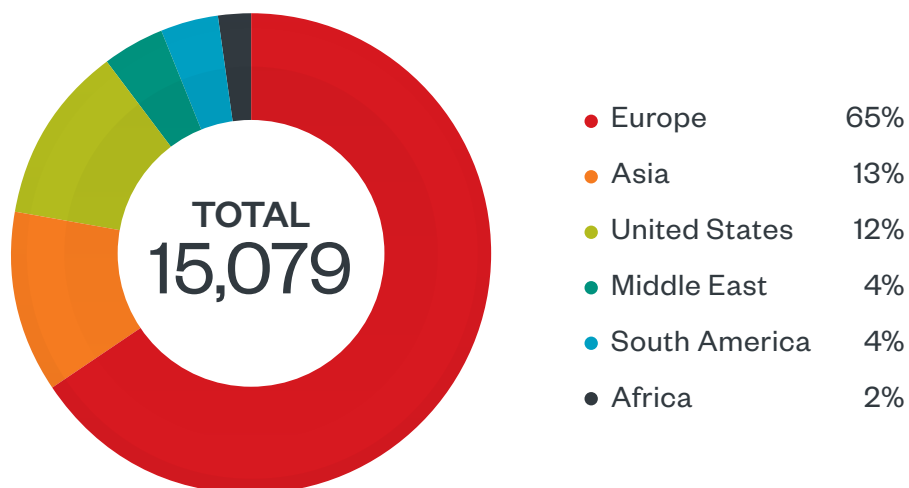


Figure 5. Breakdown of Pawn Storm's port scans on target IP address (via port 1433), by country/region

The scans were done from the IP address 185.245.85[.]178 from November to December 2019. Similarly, the exact statistics will be different for other time ranges because the targets of Pawn Storm's scanning depend on specific campaigns that have a start and an end.



# Credential Phishing Attacks via DNS SPF Requests

For over two years, we were able to observe a significant number of Pawn Storm's credential phishing campaigns through careful analysis of DNS SPF (Sender Policy Framework) requests of the domains they used. In the spring of 2017, we noticed that the Pawn Storm actors had assigned particular domain names to some of their server images. These servers were repeatedly used to send credential phishing spam emails to high-profile targets that used free webmail services.

Pawn Storm did not bother to register these domain names though, so we took the opportunity to register them and possibly get more information on their operations. We set up an infrastructure to passively log all DNS requests for the five domain names. (It is worth noting that Pawn Storm has since ceased to use these five domains since summer of 2019; the group has been using a generic server named *server[.]com* at the time of writing.)

```
X-Originating-IP: [185. .148.83]
Authentication-Results: mta4221. .bfl.yahoo.com from=e. .com; dkim=neutral (no sig)
Received: from 127.0.0.1 (EHLO [redacted].com) [185. .148.83]
  by mta4221. .bfl.yahoo.com with SMTPS; Tue, 12 Feb 2019 [redacted]
Received: from WIN-1E04K8J673N (unknown [94. .125.175])
  by [redacted].com (Postfix) with ESMTS id [redacted]
  for <[redacted]>; Tue, 12 Feb 2019 [redacted] -0500 (EST)
MIME-Version: 1.0
From: "Personal Creations" <PersonalCreations@e. .com>
To: [redacted]
Date: 13 Feb 2019 [redacted]
Subject: Time is Running Out! Shop Now for Mom and Save!
Content-Type: multipart/alternative;
```

Figure 6. Pawn Storm uses particular domain names during the EHLO command in the email protocol sessions of many of its credential phishing campaigns

Some of the domain names, which were free to register in 2017, refer to the internal naming of Pawn Storm's server images. This enabled Trend Micro to gather data on the group's credential phishing campaigns from 2017 to 2019. It appears that receiving email servers send DNS SPF requests for the domain names used in the Extended HELO (EHLO) command as part of their spam filtering algorithms.

These campaigns included spam waves against two U.S.-based free webmail providers, one Russian free webmail provider, and one Iranian webmail provider. Pawn Storm’s continued use of the domain names also put the actor at risk of revealing some of their other operations, such as moving around their server image from one IP address to another and management tasks of the server.

Even for an advanced threat actor like Pawn Storm, it takes a lot of discipline to prevent leaks related to DNS requests outside of careful VPN connection setups that obscure their home base.

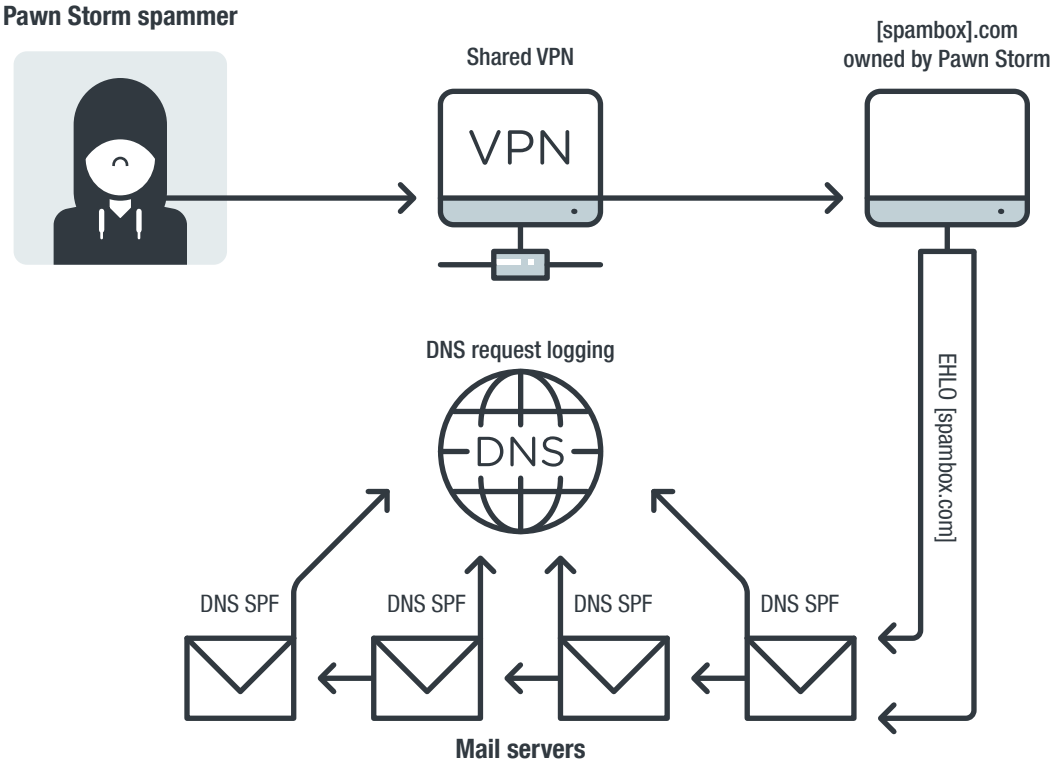


Figure 7. The setup we used to monitor Pawn Storm’s email campaigns for more than two years

Pawn Storm regularly uses the OpenVPN option of commercial VPN service providers to connect to a dedicated host that sends out spam. The dedicated spam-sending servers used particular domain names in the EHLO command of the SMTP sessions with the targets’ mail servers.

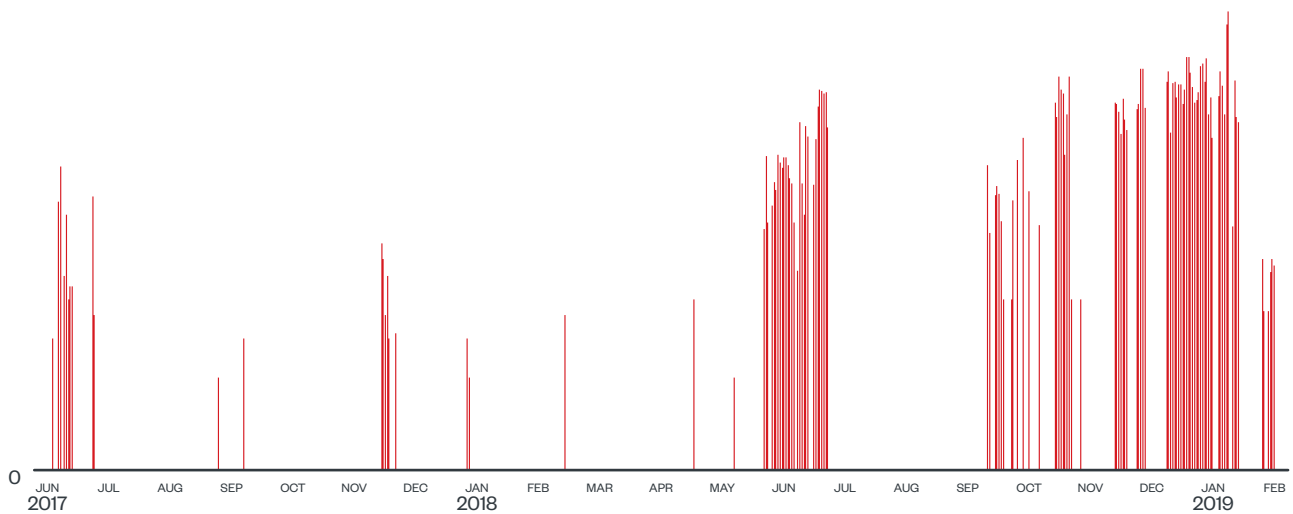


Figure 8. Yahoo phishing campaigns by Pawn Storm from late June 2017 to early March 2019

Figure 8 shows the credential phishing campaigns against Yahoo users, coming from a particular server image owned by Pawn Storm. It is measured by incoming DNS SPF requests. The vertical axis uses a logarithmic scale.

We could correlate the statistics of email campaigns derived from our DNS monitoring with the email samples we gathered over the years. Although our dataset of actual emails is smaller, the two datasets were consistent with each other.

# Conclusion and Security Recommendations

If our previous reports on Pawn Storm is any indication, the threat actor group has plenty of resources that allow them to run lengthy campaigns, determined in the pursuit of their targets. Their attacks, which range from compromising DNS settings and tabnabbing<sup>4</sup> to creating watering holes and taking advantage of zero-days,<sup>5</sup> have been nothing short of sophisticated. And as evidenced by their recent activities, we expect even more direct attacks against webmail and cloud services that don't rely on malware.

We have seen Pawn Storm's activities since 2004, and we expect the threat actor group to be active for years to come. Since Pawn Storm uses a wide range of tools and tactics, organizations must secure their perimeter to reduce the risks from any potential entry or jump-off points. Here are some measures users and organizations can take to defend against Pawn Storm's methods:

- **Enforce the principle of least privilege.** Minimize risks in the network by limiting traffic, enabling only the services needed, and disabling those that are outdated or unused.
- **Mind the security gaps.** Keep the system updated and its applications patched, create strong patch management policies, and consider virtual patching<sup>6</sup> for known and unknown vulnerabilities.
- **Regularly monitor the infrastructure.** Aside from employing firewalls, incorporate intrusion detection and prevention systems that inspect traffic in real-time and automatically remediate vulnerable systems.<sup>7</sup>
- **Require two-factor authentication.** Corporate email accounts, network access, and outsourced services should have multiple authentication measures when used.
- **Educate employees.** Raise awareness of phishing techniques and common attack vectors and prohibit the use of personal webmail and social media accounts for work purposes.
- **Maintain data integrity.** Regularly back up data and encrypt stored sensitive information.

# Indicators of Compromise (IoCs)

IP addresses	First	Last	Activity
185.245.85[.]178	8/4/19	12/17/19	Phishing; scanning for port 445 and 1433
81.19.210[.]149	5/22/19	9/20/19	Spam; scanning (webmail)
82.118.242[.]171	10/1/19	12/9/19	Scanning (webmail)
172.111.161[.]232	9/26/19	10/7/19	Spam
89.238.178[.]14	9/20/19	12/9/19	VPN use
185.227.68[.]214	12/1/19	2/18/20	Phishing and scanning

Domains	Activity
0xf4a54cf56[.]tk	Credential phishing
0xf4a5[.]tk	Credential phishing
id24556[.]tk	Credential phishing
546874[.]tk	Credential phishing
id6589[.]com	Credential phishing
id451295[.]com	Credential phishing
change-password[.]ml	Credential phishing
0x4fc271[.]tk	Credential phishing
yahoo-change-password[.]com	Credential phishing



# References

- 1 Trend Micro. (n.d.) *Trend Micro Threat Encyclopedia*. “TROJ\_SCONATO.A.” Last accessed on 4 February 2020 at [https://www.trendmicro.com/vinfo/us/threat-encyclopedia/archive/malware/troj\\_sconato.a](https://www.trendmicro.com/vinfo/us/threat-encyclopedia/archive/malware/troj_sconato.a).
- 2 Loucif Kharouni, Feike Hacquebord, Numaan Huq, Jim Gogolinski, Fernando Mercês, Alfred Remorin, and Douglas Otis. (22 October 2014). *Trend Micro Security News*. “Pawn Storm Espionage Attacks Use Decoys, Deliver SEDNIT.” Last accessed on 4 February 2020 at <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/pawn-storm-espionage-attacks-use-decoys-deliver-sednit>.
- 3 Feike Hacquebord. (25 April 2017). *Trend Micro Security News*. “From Espionage to Cyber Propaganda: Pawn Storm’s Activities over the Past Two Years.” Last accessed on 4 February 2020 at <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/espionage-cyber-propaganda-two-years-of-pawn-storm>.
- 4 Feike Hacquebord. (24 October 2014). *Trend Micro*. “Operation Pawn Storm: Putting Outlook Web Access Users at Risk.” Last accessed on 12 February 2020 at <https://blog.trendmicro.com/trendlabs-security-intelligence/operation-pawn-storm-putting-outlook-web-access-users-at-risk/>.
- 5 Feike Hacquebord and Stephen Hilt. (9 November 2016). *Trend Micro*. “Pawn Storm Ramps Up Spear-phishing Before Zero-Days Get Patched.” Last accessed on 12 February 2020 at <https://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-ramps-up-spear-phishing-before-zero-days-get-patched/>.
- 6 Trend Micro. (25 October 2018). *Trend Micro Security News*. “Virtual Patching: Patch Those Vulnerabilities before They Can Be Exploited.” Last accessed on 12 February 2020 at <https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/virtual-patching-patch-those-vulnerabilities-before-they-can-be-exploited>.
- 7 Trend Micro Incorporated. (n.d.). *Trend Micro*. “Intrusion Prevention.” Last accessed on 12 February 2020 at [https://www.trendmicro.com/en\\_us/business/capabilities/intrusion-prevention.html](https://www.trendmicro.com/en_us/business/capabilities/intrusion-prevention.html).



## TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threats techniques. We continually work to anticipate new threats and deliver thought-provoking research.

[www.trendmicro.com](http://www.trendmicro.com)



©2020 by Trend Micro, Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, and Trend Micro Smart Protection Network are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.