Two Years of Pawn Storm

Examining an Increasingly Relevant Threat

Feike Hacquebord

Forward-Looking Threat Research (FTR) Team

A **TrendLabs**SM Research Paper

Contents

4
False Flag Operations

8
How Pawn Storm Attacks Free and Corporate Webmail

19
Pawn Storm Phishing Campaigns

29
Preferred Attacks, Resources, and Tools

37
Conclusion and Defending Against Pawn Storm

Pawn Storm is an active cyber espionage actor group that has been very aggressive and ambitious in recent years. Pawn Storm's activities show that foreign and domestic espionage and influence on geopolitics are the group's main motives, and not financial gain. Its main targets are armed forces, the defense industry, news media, politicians, and dissidents. All of Pawn Storm's targets have one thing in common: they might be perceived as a risk to the current regime of Russia. We can trace activities of Pawn Storm back to 2004[1]. Before our initial report in 2014[2] there wasn't much published about this actor group. Since our paper in 2014 we published more than a dozen posts on Pawn Storm, detailing various aspects of Pawn Storm's attacks and its methodologies.[3]

Recently, Pawn Storm is becoming increasingly relevant particularly because it is doing more than just espionage. In 2016, Pawn Storm attempted to influence public opinion, to influence elections, and sought contact with mainstream media with some success. Earlier, Pawn Storm may seem to have limited their activities to political, military and domestic espionage. Today the impact can be felt by various industries and enterprises operating throughout the world. Even the average citizen of different countries might be impacted as Pawn Storm tries to manipulate people's opinions about domestic and international affairs. The attacks of Pawn Storm could serve as an example for other actors, who could copy tactics and repurpose them to fit their own objectives.

As we look at Pawn Storm's operations over a two-year period, we can see how the group has become more adept at manipulating events and public opinion through the gathering and controlled release of information. Many events—like their involvement in the Democratic National Convention hack—have been covered extensively. The group's cyber propaganda methods—using electronic means to influence opinion[4]—creates problems on multiple levels. Aside from manipulating the public, their operations also discredit political figures. The political climate in 2017, with the prevalence of fake news and fake news accusations, can in part be attributed to constant information leaks and manipulations by malicious actors. Media sources have already confirmed that Pawn Storm offered them exclusive peeks at high-impact information, presumably in an attempt to skew public perception on a certain topic or person.

In this paper, we take a deeper look at the facts we have compiled, particularly the methodologies Pawn Storm is using. Pawn Storm is known for using sophisticated social engineering lures, efficient credential phishing, zero days, a private exploit kit, an effective set of malware, false flag operations and campaigns to influence the public opinion about political issues.

At its core, Pawn Storm—also known as Sednit5, Fancy Bear, APT286 7, Sofacy, and STRONTIUM8—is a persistent cyber espionage actor group. The actors often attack the same target from different sides and they don't give up easily, using multiple methods to reach their goals. Pawn Storm generally relies on their practiced techniques, specifically when it comes to phishing. Credential phishing has been a key part of many compromises done by Pawn Storm in recent years and we were the first to describe them in detail from 2014 and onwards.

We start this paper with a section on false flag operations and a rundown of Pawn Storm's attempts to influence the public opinion. The second section focuses on different methods used to attack free and corporate webmail—mostly through sophisticated phishing tactics. Our third section details Pawn Storm's campaigns that we tracked over the years, and lists their intended targets. The next section covers their preferred attacks, facilitators, and also their attitude towards their own operational security. And lastly, we give some guidelines on how to protect yourself from Pawn Storm.

False Flag Operations

Pawn Storm uses a variety of tactics to collect information from their identified targets—often through credential phishing. Some of the information is then leaked on websites that are specifically designed to display stolen data. More than once Pawn Storm disguised itself as "hacktivists" or whistleblowers motivated by some agenda.

Operating Under Alternative Fronts

For example after Pawn Storm breached the World Anti-Doping Agency (WADA) and the Court of Arbitration for Sport (TAS-CAS) in 2016, a group that calls themselves the "Fancy Bears' Hack team" posted medical records of athletes on their website (security company CrowdStrike uses "Fancy Bear" to identify Pawn Storm actors). The hack team claims they "stand for fair play and clean sport", however, in reality they leak confidential medical records that were very likely stolen by Pawn Storm. This move could be meant as retaliation against the decision of WADA to block some Russian athletes from the Olympics in Rio de Janeiro, Brazil. It could also be meant to weaken the position of WADA and influence the public opinion of doping incidents.

In 2015 Pawn Storm released information of the US Army on the site cyb3rc.com using the Cyber Caliphate front. The group presented itself as pro-ISIS and suggested that they are an Islam-inspired terrorist group. In the same year, Cyber Caliphate claimed to have taken down the live broadcasting of French TV station TV5 for a number of hours. Also, pro-ISIS messages from the group appeared on the Twitter and Facebook accounts of TV5. This was particularly painful for France, a country that was still in shock from terrorist attacks on the editors of Charlie Hebdo, a French satirical weekly magazine. However, it was later reported that the Cyber Caliphate was a front of Pawn Storm.

French magazine L'Express shared indicators with us that clearly pointed to Pawn Storm, which French authorities later confirmed. The motives for the TV5 attack are still unclear. Maybe the actors wanted to show that they are capable of compromising a TV station. Maybe they wanted to cause PR damage, like when they took over the Twitter account of Newsweek and the US Central Command earlier in 2015. Maybe this was the way Pawn Storm actors were attempting to destabilize France as a nation.

Of course, it is also possible there is no real good explanation and this attack was the work of undisciplined Pawn Storm actors. The fact that Pawn Storm posed as terrorists was particularly harsh and doesn't fit with their usual espionage campaigns and information-gathering activities. Though the Pawn Storm actors normally work in a professional way, there have been a few other incidents that showed lack of discipline among some of the Pawn Storm actors.

Maneuvers Used Against Political Organizations

In 2016 the Democratic National Committee (DNC) was allegedly hacked by Pawn Storm. Stolen emails were published by Wikileaks and a site called dcleaks[.]com—a domain very likely controlled by Pawn Storm. After the DNC hack became public, a supposedly lone hacker called Guccifer 2.0 claimed responsibility. He claimed to be Romanian (just like the real hacker Guccifer who was convicted in 2016 for compromising the email accounts of American business executives, political figures and celebrities), but while communicating with the press, it appeared that Guccifer 2.0 was not fluent in Romanian at all.

A study of ThreatConnect[9] showed that the Guccifer 2.0 hacker approached news media and offered them exclusive access to password protected parts of the dcleaks[.]com site. This specific site actually leaks email repositories of mainly US Pawn Storm targets that have been victimized by their advanced Gmail credential phishing campaigns. We were able to collect a substantial amount of information on the Gmail credential phishing campaigns of Pawn Storm from 2014 onwards (as we describe on page 18). This makes it very likely that Guccifer 2.0 is a creation of the Pawn Storm actor group.

It is very plausible that Pawn Storm also supplied the Wikileaks organization with stolen information. Wikileaks, which has dubbed itself a "multi-national media organization and associated library", published emails from the DNC and the AK party of Turkish President Erdogan in 2016. We know that the DNC received a wave of aggressive credential phishing attacks from Pawn Storm in March and April 2016. During the campaign, dozens of politicians, DNC staff, speech writers, data analysts, former staff of the Obama campaign, staff of the Hillary Clinton campaign, and even corporate sponsors were targeted multiple times. Pawn Storm also attacked the Turkish government and parliament in early 2016. This makes it highly plausible that the DNC emails that were published by Wikileaks were originally stolen by the Pawn Storm actor group.

Utilizing Mainstream Media

There have been instances when Pawn Storm uses mainstream media to publicize their brazen attacks and influence public opinion. Several media outlets have confirmed that they were offered exclusive access to data stolen by Pawn Storm. One particular example is the reputable German magazine Der Spiegel that reported on doping in January 2017[10]. Der Spiegel wrote they were in contact with the "Fancy Bear hackers" for months and that in December 2016 they received "several sets of data containing PDF and Word documents in addition to hundreds of internal emails from USADA and WADA, the World Anti-Doping Agency." This is a clear example where Pawn Storm successfully contacted mainstream media to influence the public opinion about a political topic.

The reports on the Democratic Congressional Campaign Committee (DCCC) being compromised by Russian hackers, published at end of July 2016, serve as another example. More than five weeks before the DCCC compromise became public, we discovered that the website was severely compromised. All donations meant for dccc.org were first redirected to a site that was under Pawn Storm's control—this means that the actors had the opportunity to compromise donors of the Democratic Party. At the time of discovery, the compromise was about a week old and was still live. We disclosed the compromise to US authorities responsibly and the problem was addressed quickly. We did not publish our findings as a public report could actually benefit Pawn Storm by highlighting their capabilities and also impacting the US elections. But then more than five weeks later the compromise did make headlines. Pawn Storm possibly contacted mainstream media about the compromise and, just like in other cases, offered "exclusive" access to stolen information.

Phishing and Things Pawn Storm Can Do with the Data

In April and May 2016 Pawn Storm launched attacks against the German political party Christian Democratic Union (CDU) headed by Angela Merkel, which is also around the same time the group set up phishing sites against two German free webmail providers[11]. German authorities later confirmed that this attack was the work of Pawn Storm. However we don't know whether they were successful or not. No emails of CDU have been leaked yet, but in some instances Pawn Storm has waited for more than a year before it started to leak stolen data.

In early 2016, Pawn Storm also set up credential phishing sites that targeted ministries of the Turkish government and the Turkish parliament[12]. While in October 2016 a credential phishing site was set up to target the parliament of Montenegro—this was highly likely the work of Pawn Storm too.

Pawn Storm has also probably leaked stolen information via cyber-berkut[.]org. This is the website of an actor group posing as a pro-Russian activist group that has a particular interest in leaking documents from the Ukraine. We don't know the exact relation between Pawn Storm and CyberBerkut, but we have

credible information that CyberBerkut has published information which was stolen during credential phishing campaigns of Pawn Storm. Prior to leaking the info, parts of the documents and emails were allegedly altered.

Generally, the authenticity of leaked data is not verified. This leaves room for threat actors to alter the stolen data to their own benefit and present it as real and unaltered. By publishing carefully selected pieces of unaltered stolen data, threat actors can even more effectively influence public opinion in a way that is aligned with their interests.

The incidents mentioned above make it clear that Pawn Storm has a definite interest in influencing politics in different countries. This is not limited to the presidential elections in the US, but goes far beyond that and started before the elections happened. In the next sections we will explain in more detail why credential phishing has been so effective for Pawn Storm.

How Pawn Storm Attacks Free and Corporate Webmail

Credential Phishing

Credential phishing is an effective tool in espionage campaigns. A lot of Internet users are trained by experience not to fall victim to phishing. They are trained to spot obvious grammar and spelling errors, uncommon domains in the phishing URLs and the absence of a secure, encrypted connection in the browser bar. However, professional actors have the resources to avoid simple mistakes and invent clever social engineering tactics. They send phishing emails in flawless English and other languages when needed, and they have no problem evading spam filters.

Essentially, credential phishing attacks have become an effective and dangerous tool that can have severely damaging effects. In these attacks a huge amount of sensitive data might be stolen. Credential phishing also serves as the first step to penetrate deeper into the infrastructure of a victim organization.

Several attack scenarios are possible through credential phishing:

- silent data gathering over an extended period of time—Pawn Storm being a prime example since our data tracks them silently collecting information for more than a year
- compromised accounts are used to further penetrate into the network of a victim organization, for example by sending emails using stolen identities
- leaking sensitive emails in order to cause harm to the victim organization and influence public opinion
- domestic espionage on citizens of nations

Pawn Storm is doing all of the above. With relatively simple, but oftentimes well-prepared credential

phishing, Pawn Storm has been able to collect an enormous amount of data. In 2016 Pawn Storm is believed to have stolen information from the DNC, Hillary Clinton's campaign team, and WADA. They also launched credential phishing attacks on numerous other organizations: armed forces, defense companies, media, and many others.

It is very likely that from July 2015 to August 2016, Pawn Storm had access to the Gmail account of Colin Powell, former United States Secretary of State under the George Bush administration. In September 2016, more than one year after the initial compromise, dcleaks[.]com posted several of his personal emails online. This was just one of the many examples where Pawn Storm leaked confidential information, and it shows that some of the compromises span a lengthy period.

Russian citizens, like activists, journalists and dissidents, are constantly targeted by Pawn Storm[13]. While some dissidents only seem to shrug their shoulders, it can have real consequences and negatively affect people's lives. Several Russian media organizations have been spied on by Pawn Storm, even a mainstream media corporation that is not particularly critical of the current regime. Software developers, politicians, researchers at universities, and artists in Russia have also been frequent targets of Pawn Storm. Foreign embassies in Moscow are common targets too.

Pawn Storm has maintained long-running campaigns against high profile users of free international webmail providers like Yahoo and Gmail; as well as webmail providers for Ukrainian Internet users (Ukr.net), and Russian users (Yandex and Mail.ru). Pawn Storm sets up phishing sites of other free webmail providers for very specific targets only. We found Pawn Storm phishing domains for relatively small webmail providers in Cyprus, Belgium, Italy, Norway, and other countries. Users of university webmail in Estonia and Russia were targeted as well. These were probably part of tailored attacks where Pawn Storm had very specific and high-profile targets in mind.

The credential phishing attacks against high profile Google, Yahoo and Ukr.net users are relatively voluminous. We were able to collect thousands of phishing emails since early 2015. It was not continuous—Pawn Storm sometimes paused activities, but then later on resumed. Some targets get multiple phishing emails in one week.

Credential Phishing Attacks on Corporate Webmail

In the last four years Pawn Storm has launched numerous credential phishing attacks against the corporate email system of many organizations. Targets included armed forces, defense industry, political parties, NGOs, media, and governments around the world. Attacking corporate email makes a lot of sense for actors like Pawn Storm as email is one of the weakest points in the targets' defense. Breaching corporate email accounts may lead the actors to interesting, confidential data and it can be a stepping stone that allows for penetrating deeper into the target organization.

Many organizations allow their employees to read email while they are out of the office. While this greatly enhances user convenience, webmail introduces significant risks. Webmail that can be accessed from anywhere introduces an attack surface that can be probed not only by direct hacking, but also by advanced social engineering. While people might be used to less sophisticated credential phishing emails, advanced actors have shown remarkable creativity in their attacks and often they are fluent in foreign languages as well. For some of the attacks, victims cannot be blamed for falling for the social engineering tricks. We have seen phishing lures that are almost indistinguishable from legitimate emails. One of the social engineering lures makes use of a form of tabnabbing, which is discussed below.

Here are some considerations on the security of webmail:

- Two-factor authentication increases security, but it doesn't make social engineering impossible. All temporary tokens can be phished by an attacker.
- Even when two-factor authentication is used, an attacker only has to phish for the second authentication token one or two times to get semi-permanent access to a mailbox. They can set up a forwarding address or a token that allows third party applications full access to the system.
- Mandatory logging in onto a company VPN network does raise the bar for an attacker. However, VPN credentials can also be phished, and we've seen targeted attackers specifically go after VPN access credentials.
- Authentication with a physical security key makes credential phishing virtually impossible unless the attacker has physical access to the equipment of the target. When a target uses a physical security key, the attacker either has to find an exploit to get unauthorized access, or he has to get physical access to the security key and the target's laptop.
- To add to authentication methods that are based on what you know and what you have, one could add authentication that is based on what you are: fingerprints or other biometric data. Biometrics have already been used by some laptops and phone vendors, and have also been a common authentication method in datacenters for more than a decade.

Phishing Campaign Targets

This section lists some of the organizations that were targeted by Pawn Storm with a campaign that was specifically set up for them. In many cases, only very few employees of these organizations were targeted.

Date	Organization	Phishing domain
Military		
12/12/13	Chilean military	mail.fach.rnil.cl
05/15/14	Armenian military	mail.rnil.am
10/23/14	Latvian military	web.mailmil.lv
02/25/15	Romanian military	fortele.ro
03/25/15	Danish military	webmail-mil.dk
03/26/15	Portuguese military	webmail.exerclto.pt
05/13/15	Greek military	webmail-mil.gr
09/04/15	Danish military	fkit-mil.dk
09/05/15	Saudi military	mail.rsaf.qov.sa.com
10/16/15	United Arab Emirates army	mailmil.ae
10/19/15	Kuwaiti military	mail.kuwaitarmy.gov-kw.com
10/21/15	Romanian military	mail-navy.ro
03/04/16	Bulgarian army	mail.armf.bg.message-id8665213.tk
Ministry of Defense (MOD)		
01/23/14	MOD Bulgaria	mail.arnf.bg
02/11/14	MOD Poland	poczta.mon.q0v.pl
04/04/14	MOD Hungary	mail.hm.qov.hu
04/30/14	MOD Albania	mod.qov.al
05/22/14	MOD Spain	mail.mod.qov.es
11/18/14	MOD Afghanistan	mail.mod.qov.af
09/05/15	MOD Saudi Arabia	mail.moda.qov.sa.com
02/19/16	MOD Poland	poczta.mon-gov.pl
Ministry of Foreign Affairs (MFA)		
03/17/15	MFA South Georgia	email.mfa.qov.gs
07/16/15	MFA Armenia	webmail-mfa.am
10/02/15	MFA United Arab Emirates	webmail.mofa.qov.ae
10/02/15	MFA United Arab Emirates	webmail.mfa.qov.ae
12/10/15	MFA Qatar	mail.mofa.g0v.qa

Date	Organization	Phishing domain
Intelligence Units		
01/10/14	National Security Bulgaria	dansa.bg
Defense Industry		
04/24/14	Academi	mail.academl.com
04/24/14	Boston Dynamics	mail.bostondynamlcs.com
08/11/14	Science Applications International Corporation (SAIC)	webmail-saic.com
09/10/14	Polski Holding Obronny	mailpho.com
Media		
11/01/14	New York Times	privacy-yahoo.com
12/01/14	New York Times	link.candybober.info
01/22/15	Buzzfeed	account.password-google.com
06/22/15	The Economist Intelligence Unit	accounts.g00qle.com
08/24/15	Sanoma Media	mobile-sanoma.net
02/24/16	Hurriyet	posta-hurriyet.com
03/14/16	Anadolu Agency	anadolu-ajansi.com
03/15/16	Anadolu Agency	mail.anadoluajansi.web.tr
05/11/16	Hurriyet	webmail-hurriyet.com
06/12/16	Hurriyet	mail-hurriyet.com
11/14/16	Al Jazeera	account-aljazeera.net
11/14/16	Al Jazeera	ssset-aljazeera.net
11/15/16	Al Jazeera	sset-aljazeera.net
11/16/16	Al Jazeera	sset-aljazeera.com
11/21/16	Al Jazeera	mail-aljazeera.net
Political Parties		
03/01/15	National Democratic Institute	url.googlesetting.com
04/01/15	National Democratic Institute	login.accoounts-google.com
01/12/16	Prime Minister Turkey	e-post.byegm.web.tr
01/12/16	Prime Minister Turkey	mail.byegm.web.tr
02/01/16	Prime Minister Turkey	eposta.basbakanlik.qov.web.tr
02/01/16	Parliament Turkey	e-posta.tbmm.qov.web.tr
03/01/16	Democratic Party US	myaccount.google.com-securitysettingpage.gq

Date	Organization	Phishing domain
04/01/16	Democratic Party US	myaccount.google.com-changepasswordmyaccount-idx8jxcn4ufdmncudd.gq
04/22/16	CDU	webmail-cdu.de
05/06/16	CDU	support-cdu.de
06/06/16	Democratic Party US	actblues.com
10/20/16	parliament Montenegro	mail-skupstina.me
Religion		
06/19/15	Orthodox Church America	accounts.g00qle.com
Academics		
03/04/16	Tartu University	mail.university-tartu.info
09/13/16	Baikal State University	mail-isea.ru
Government Agencies		
05/24/15	Government of Montenegro	mail-gov.me
09/14/15	Safety Board Netherlands	vpn.onderzoekraad.nl
09/28/15	Safety Board Netherlands	sftp.onderzoekraad.nl
09/29/15	Department of Civil Aviation Malaysia	mail.dca.qov.my
11/03/15	Government of Montenegro	mail.g0v.me
Energy Sector		
12/10/14	Westing House Nuclear	webmail.westinqhousenuclear.com
International Organisations		
06/18/14	Organization for Security and Co-operation in Europe (OSCE)	login-osce.org
04/23/15	Partnership for Peace Information Management System	mail-pims.org
08/03/16	World Anti-Doping Agency (WADA)	mail.wada-awa.org
08/08/16	World Anti-Doping Agency (WADA)	inside.wada-arna.org
08/08/16	Tribunal Arbitral du Sport (TAS, Court of Arbitration for Sport)	tas-cass.org

Table 1. Table showing the targeted organizations and specific sites set up to target them

Tabnabbing in Credential Phishing

Tabnabbing is a term that was originally introduced by researcher Aza Raskin[14]. He describes the attack as follows: a URL in an open tab of the browser is changed to a phishing site when simple JavaScript detects that the user has moved on to another tab or is inactive for some time. When the target believes that the phishing site is the real login site of the Internet service he was using, he might reenter his credentials on the phishing site.

The trick exploits Internet users' habit of keeping several tabs open in their browser for an extended period of time. Many services like online banking require reentering credentials after a certain period of inactivity so the user might be familiar with this routine.

Pawn Storm has been using a variant of tabnabbing[15]. In this attack scenario, the target gets an email supposedly coming from a website he might be interested in—maybe from a conference he is likely to visit or a news site he has subscribed to. The email has a link to a URL that looks very legitimate. When the target reads his email and clicks on the link, it will open in a new tab. This new tab will show the legitimate website of a conference or news provider after being redirected from a site that is under the attackers' control. The target is likely to spend some time browsing this legitimate site. Distracted, he probably did not notice that just before the redirection, a simple script was run that changed the original webmail tab to a phishing site. When the target has finished reading the news article or conference information on the legitimate site, he returns to the tab of his webmail. He is informed that his session has expired and the site needs his credentials again. He is then likely to reenter his password and give his credentials away to the attackers.

This attack scenario is very simple and no exploits are being used. Its success depends on good preparation by the attacker, but even experienced security researchers could fall for this social engineering trick, in particular when they are on the road and not paying attention to every detail.

In Table 2 we show some examples of organizations that have been targeted with credential phishing attacks that made use of this tabnabbing trick.

Target Organization	Phishing domain	Malicious Domain (Social Lure)	Real Domain
Academi	mail.academl.com	tolonevvs.com	tolonews.com
Armed forces Latvia	mailmil.lv	tusexpo2015.com	tusexpo.com
imperialconsult.com	mail.imperialc0nsult.com	skidkaturag.com	skidkatur.com
MOD Hungary	mail.hm.gov.hu	aadexpo2014.co.za	adexpo.co.za
MOD Hungary	mail.hm.gov.hu	itec2014.co.uk	itec.co.uk
MOD Hungary	mail.hm.gov.hu	sofexjordan2014.com	sofexjordan.com

Target Organization	Phishing domain	Malicious Domain (Social Lure)	Real Domain
MOD Hungary	mail.hm.gov.hu	eurosatory2014.com	eurosatory.com
MOD Spain	mail.mod.gov.es	gdforum.net	gdforum.org
National Security Bulgaria	mail.dansa.bg	counterterorexpo.com	counterterrorexpo.com
National Security Bulgaria	mail.dansa.bg	novinitie.com	novinite.com
National Security Bulgaria	mail.dansa.bg	standartnevvs.com	standartnews.com
OSCE	login-osce.org	vice-news.com	news.vice.com
SAIC	webmail-saic.com	natoexhibitionff14.com	natoexhibition.org
Yahoo users	us6-yahoo.com	us6-yahoo.com	youtube.com

Table 2. Organizations that were targeted with credential phishing that made use of the tabnabbing trick (2014)

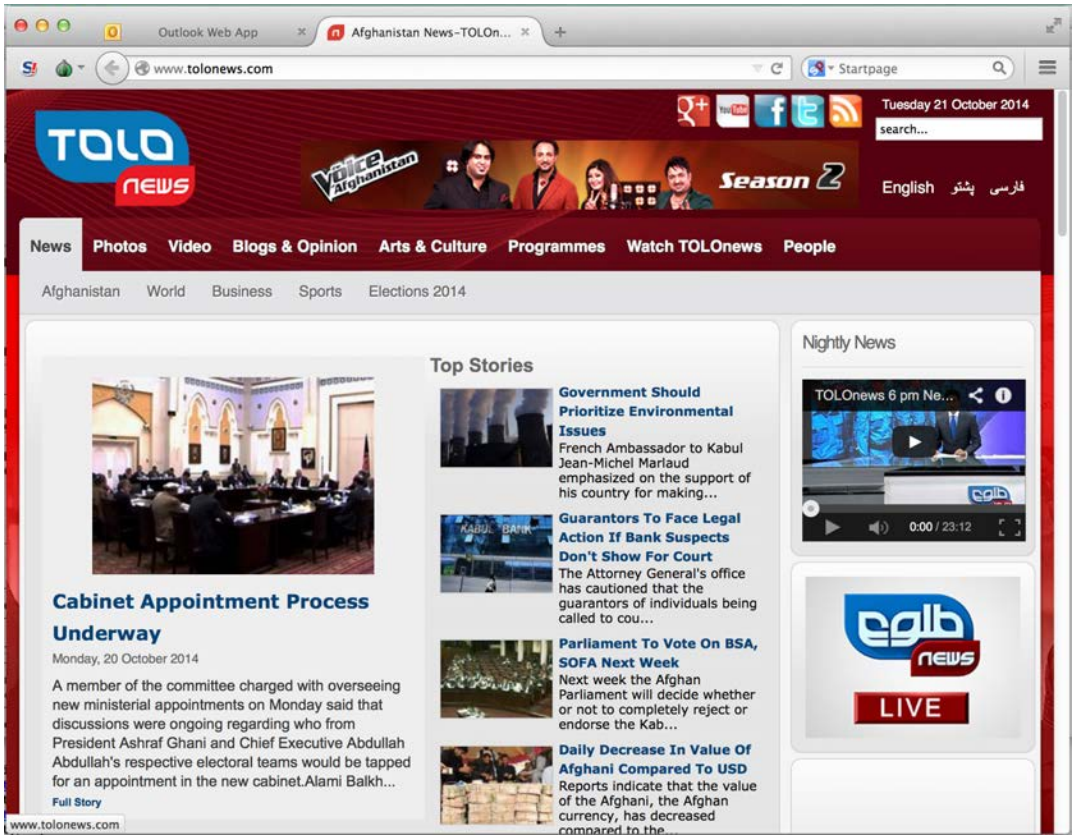


Figure 1. A target clicks on a link in an email and is redirected to a legitimate news site that will likely hold his interest

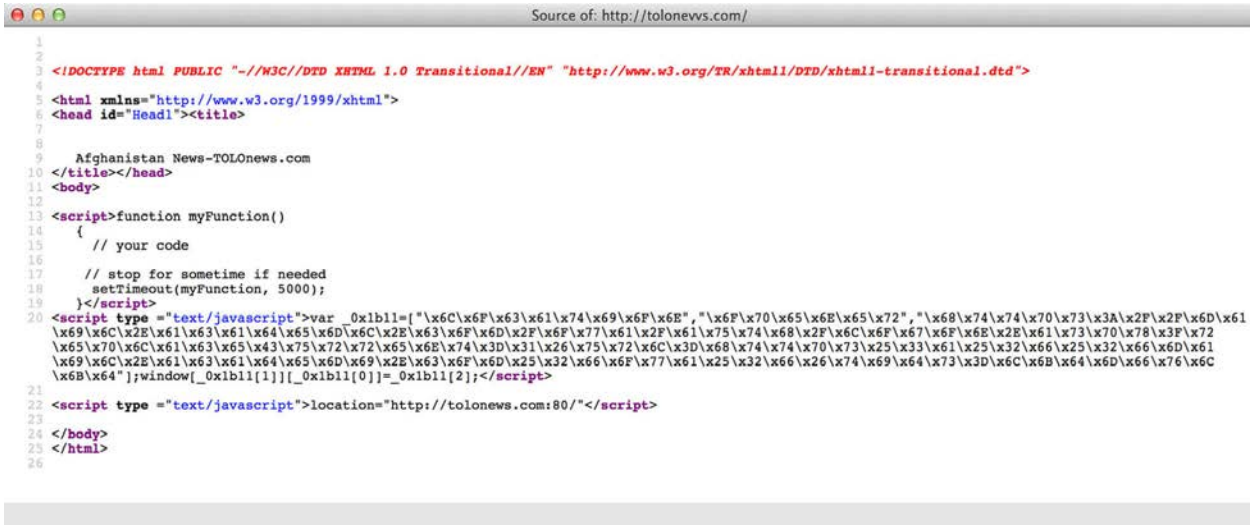


Figure 2. Simple JavaScript that is run on the Pawn Storm-controlled website, just before the user is redirected to the legitimate news site

The JavaScript is not malicious and will point the URL in the parent window to a credential phishing site.

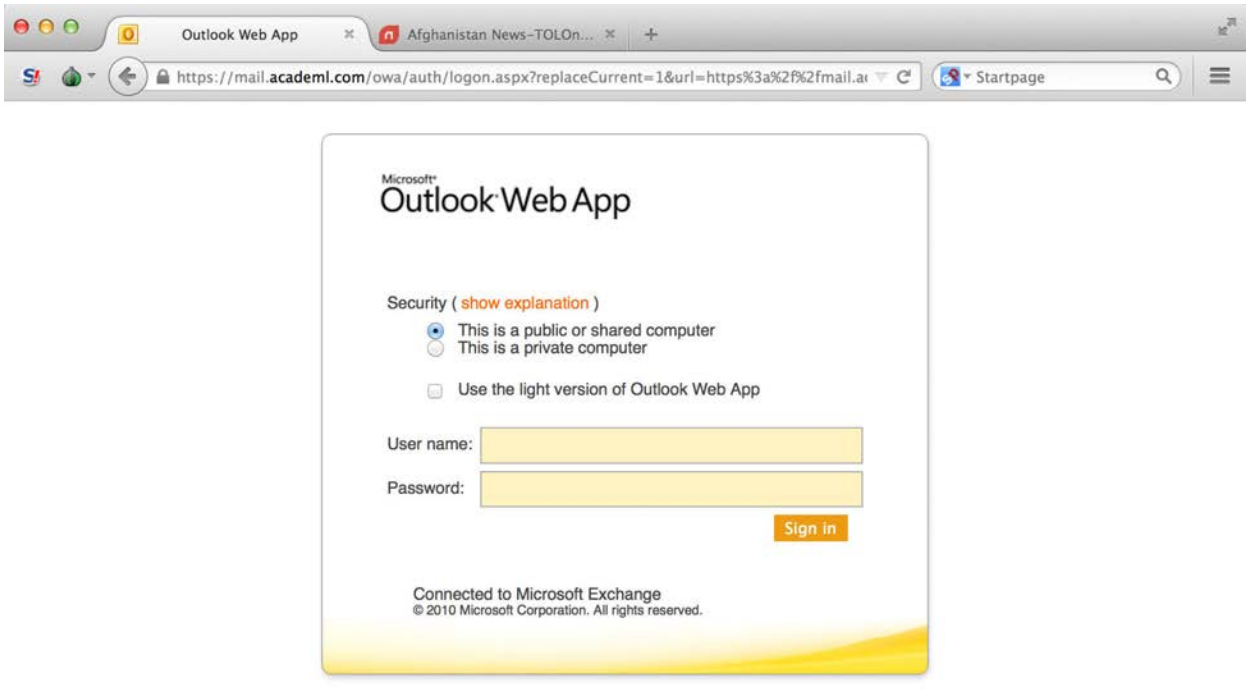


Figure 3. The credential phishing site that was opened in the browser by the tabnabbing trick

The phishing site is practically indistinguishable from the original webmail site apart from one typo in the domain. The target is very likely to fall victim to the attack.

Compromising DNS settings

In another simple but dangerous attack scenario against corporate email systems, the DNS settings of the mail servers are compromised and changed to point to a foreign server. It is not an unknown scenario, as even reputable companies have had their DNS settings compromised in the past. Often these compromises are done by hackers who want some media attention either for themselves or for a specific cause. These hacks are detected quickly and undone quickly, especially if the hackers are just seeking media attention. They simply put up a "hah, you are hacked" message or something similar on the hijacked domain. A more advanced attacker can apply the same kind of tricks, but as quietly as possible. When an attacker gets DNS admin credentials, he can modify the zone file of a domain name (note that reputable registrars offer enhanced security—changes to zone files have to be confirmed by a DNS admin over the phone). By changing the MX record of a domain to point to a proxy IP address he controls, an attacker can receive all incoming email.

The proxy can be set up to forward all incoming email to the real, actual receiving email server of the target. In this way the attacker will be able to read all metadata of incoming emails, and the contents of all emails that don't use encryption. Though this kind of attack is not advanced in nature it can have devastating consequences. We know of a Ministry of Foreign Affairs in an Eastern European country that had the MX record of their domain compromised by Pawn Storm for many months.

We warned the Ministry of Foreign Affairs about the compromise, but the process wasn't that straightforward. All of the email communications of the ministry couldn't be trusted and we did not trust in the safety of their phone system either. As a solution, we first contacted a CERT contact in Europe by phone. We described the issue and then sent the details in a PGP-encrypted email to the Western European CERT. The CERT sent a secure message to an embassy in the affected country. The embassy decrypted and printed the email. After that, a courier gave the message to the Ministry of Foreign Affairs and the issue was addressed and resolved.

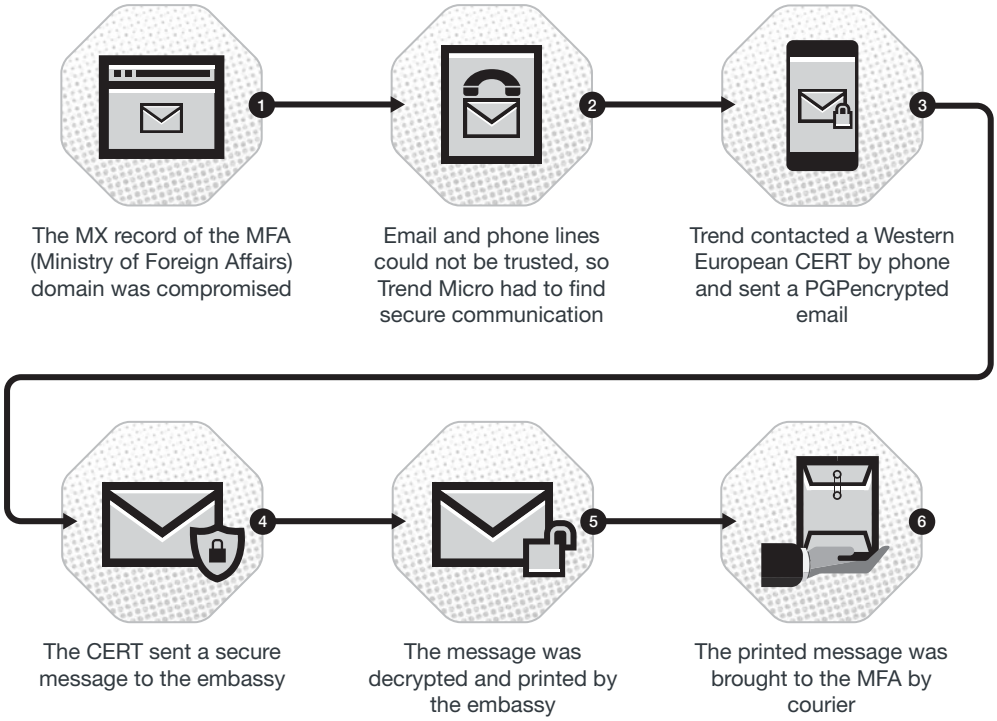


Figure 4. How Trend Micro warned the MFA about the discovered compromise

This attack scenario makes it clear that it is very important for organizations to use reputable DNS providers and registrars only, and to lock down their domain registration so that they don't get hijacked easily.

In the past there was at least one other instance where the DNS settings of a governmental institution in a West African country were compromised by Pawn Storm for a couple of months.

Pawn Storm Phishing Campaigns

Credential Phishing Campaigns

Pawn Storm is constantly trying to get access to the mailboxes of high profile users of free webmail services. We know of dozens of campaigns, each targeting up to thousands of high profile individuals. The social engineering lures used in the campaigns vary in quality, but some lures can be particularly dangerous.

In this section we show a couple of these attacks. We collected credential phishing emails that were sent by Pawn Storm to a handful of high profile Yahoo accounts from January 2015 to December 2016. The diagram below shows the distribution of more than 160 credential phishing attacks that were sent to these high profile Yahoo users.

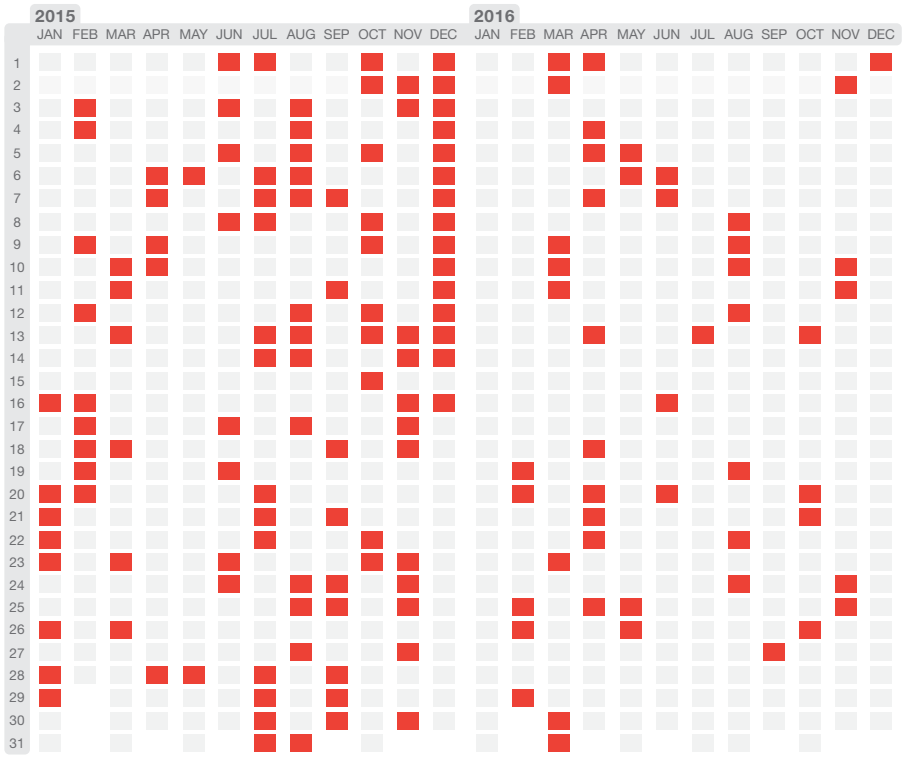


Figure 5. Distribution of Pawn Storm's 160 credential phishing attacks

The diagram shows that Pawn Storm took a long break during the holidays at the end of 2015. However, from mid-November to mid-December 2015, Pawn Storm was particularly active with credential phishing against high profile targets. Within this period, Pawn Storm was using a particularly dangerous and effective method of credential phishing we will discuss below.

A serious compromise of a target organization can start with this relatively simple credential phishing email:

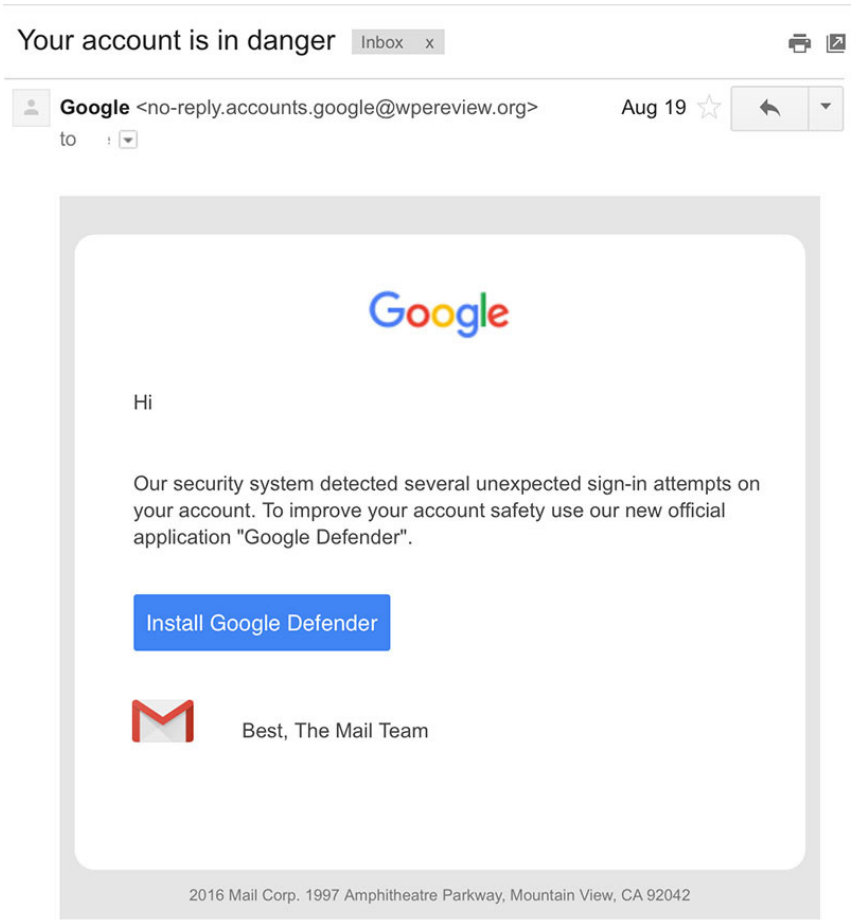


Figure 6. Email requesting installation of malicious application “Google Defender”

The email poses as an advisory from Gmail to install an "official" application called "Google Defender". Normally an internet user will be wary of installing applications he did not ask for. In this particular case however, a click on the link will lead to a page on Google.com that looks like this:

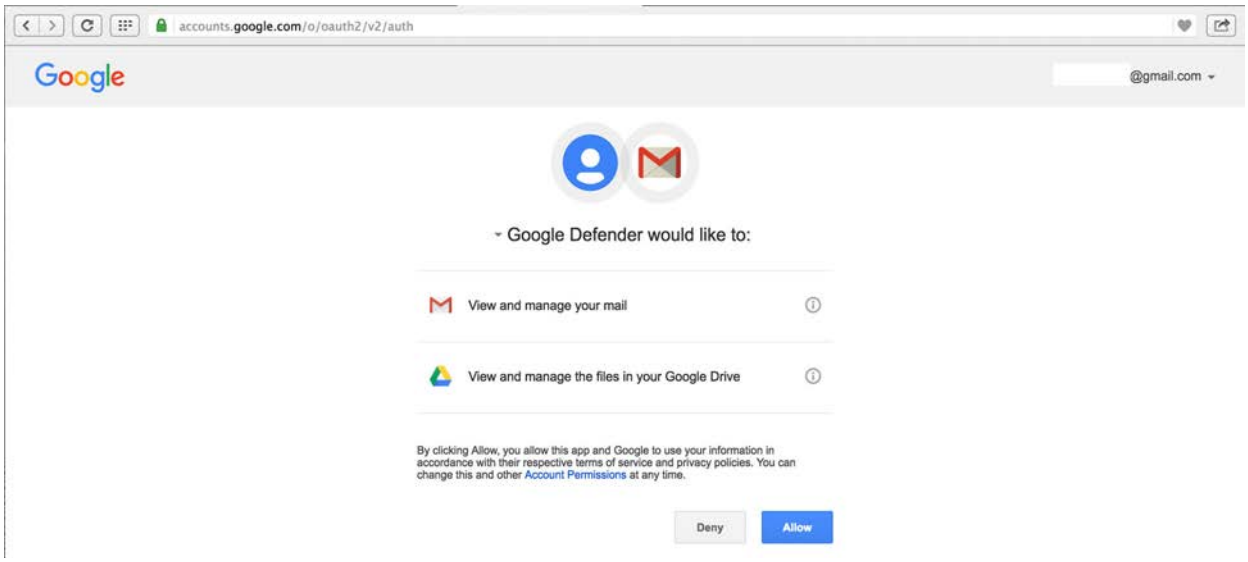


Figure 7. A legitimate-looking "Google Defender" page asking for email access permissions

At first sight this might look like a legitimate service of Google: the URL is hosted on the legitimate domain accounts.google.com, and the communication with this website is encrypted like usual. The average Internet user might actually be convinced this is all legitimate. However, despite being on accounts.google.com, the application doesn't belong to Google—it is a third party application made by Pawn Storm. In this social lure Open Authentication (OAuth), an open authentication standard, is abused. Below we will explain in more detail what OAuth is normally used for.

Similar attacks from Pawn Storm targeted high profile Yahoo users. For example in one of the late-2015 campaigns McAfee Email Protection was offered:

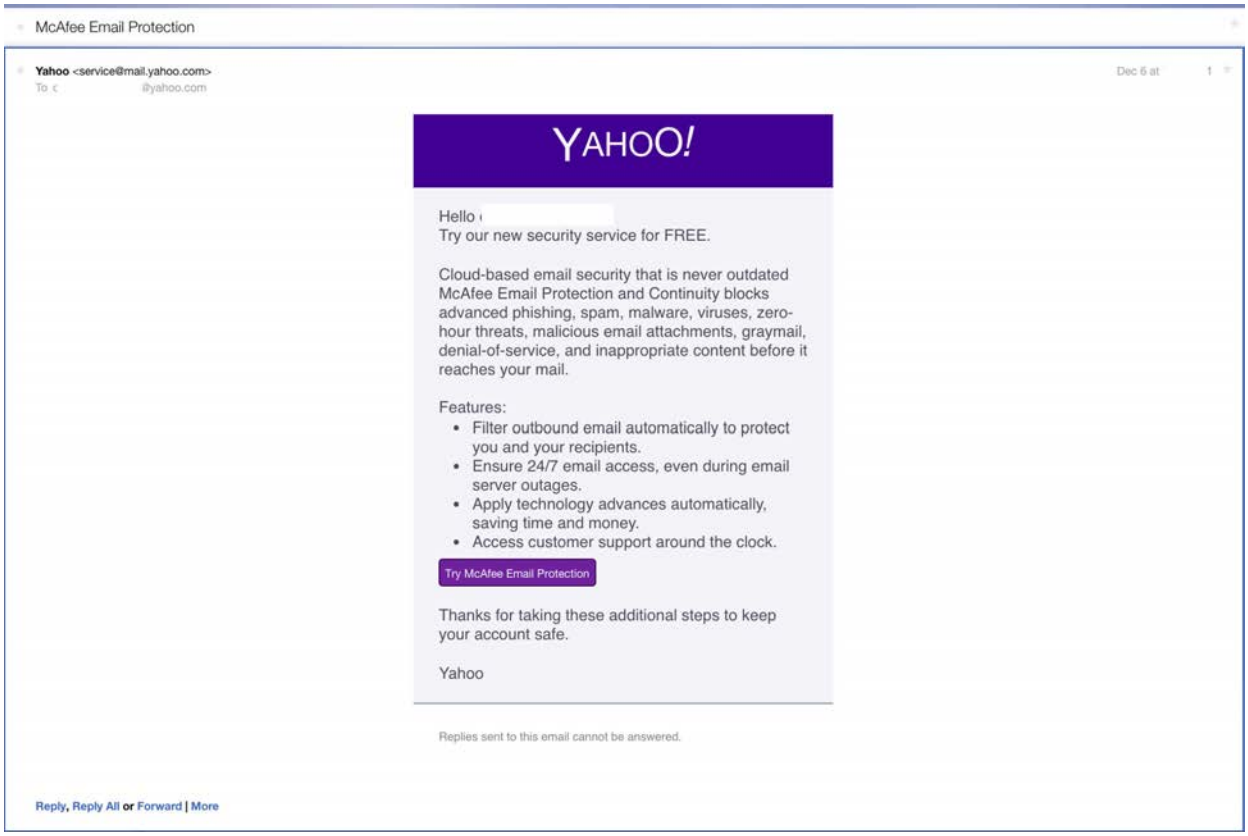


Figure 8. A phishing attack targeting high profile Yahoo users

Clicking on the phishing link would lead the target to a URL on the legitimate Yahoo domain api.login.yahoo.com. Here the user is asked to turn on "McAfee email protection" that would protect the user against various threats. When this offer is accepted, Pawn Storm actors would have full access to his email.

This lure is similar to the one that was used against Gmail users. It is particularly dangerous as most Internet users might not realize the applications are not endorsed and carefully checked by their email provider.

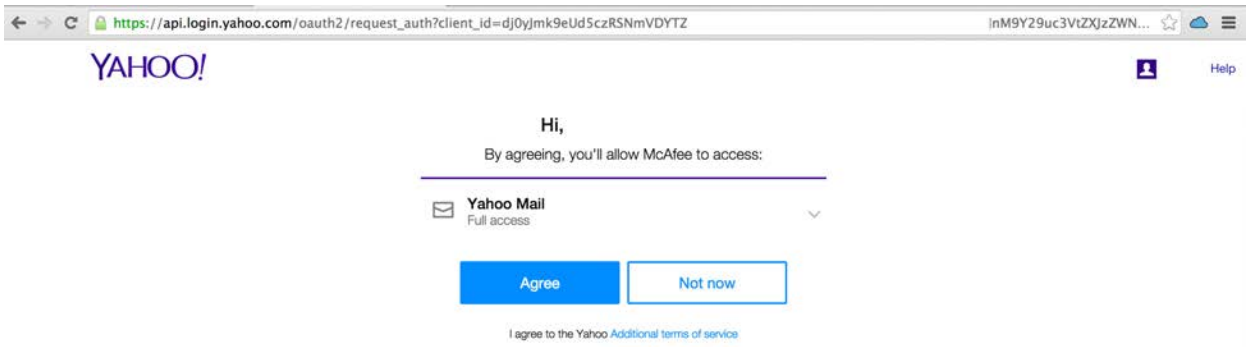


Figure 9. Pawn Storm lure for Open Authentication abuse created for Yahoo users at the end of 2015

This social engineering lure makes use of an authorization method called Open Authentication (OAuth). OAuth is a way of authorizing third party applications to login to users' online accounts for free webmail and other services. The big advantage is that users don't have to reveal their password to the third party. Instead the third party applications get a token that can be used for authentication.

OAuth is great for the users' experience on the web. For example, by allowing social networks to access your webmail contact list, it is easier to find friends who are subscribed to the same social network. Another popular use for OAuth is merging different free webmail accounts into one email account.

While OAuth offers convenience and useful applications, it also exposes the user to risks. In particular it allows for advanced social engineering schemes that take advantage of it, particularly when no good background checks are done for applications that are authorized by service providers to use OAuth. For some free webmail services an email address and a website is enough to allow a third party application to use OAuth. Because of that, OAuth abuse is straightforward and actor groups like Pawn Storm are taking advantage of OAuth for credential phishing schemes.

These attacks can have the same negative consequences as traditional credential phishing, even when no credentials are given away. The scheme is quite simple:

- an actor creates and signs up a rogue application with an online service provider—like a free webmail provider that supports OAuth
- the application passes the (basic) security checks the online service provider does to confirm whether the application is legitimate
- the actor now sends out emails to targets with a social engineering lure that would trick the recipients into allowing OAuth authentication for the rogue application
- the target might be familiar with generic phishing emails, but not so much with OAuth abuse tricks. Chances are significant that even well-educated targets get fooled

- once OAuth access has been authorized, the target account can be accessed until the user or the provider revokes the token. If the target changes his password, the actor can still use the OAuth token to access the mailbox. In this case the target might have a false sense of security.

We informally spoke with two large webmail providers that allow OAuth authentication by third party applications. As a result of our informal talks, one webmail provider has changed the way new applications are authorized to use OAuth. New applications have to go through a more thorough check before they can use OAuth. The other webmail provider was not immediately convinced that something had to be changed in their setup. As far as we know, they did not change anything, thus, users of this free webmail provider are still at a higher risk of social engineering attacks that abuse the OAuth protocol.

For the provider that changed the OAuth setup we have noted that Pawn Storm stopped sending phishing lures that abuse OAuth since late 2015. Instead Pawn Storm went back to plain old credential phishing that is generally less efficient.

For the other webmail provider that did not change the OAuth setup, Pawn Storm kept on sending targets phishing lures that abuse OAuth. Several Pawn Storm applications that were authorized to use OAuth by this free webmail provider were not removed for months. We noted that one application wasn't removed after more than 5 months. This means that high profile targets are at significant risk as the OAuth tokens that allowed Pawn Storm to silently access webmail boxes were likely not revoked either. When Pawn Storm's applications are allowed to use OAuth for such an extended period and the tokens don't get revoked, the victim is exposed and can be spied on for a long time. We have seen instances of high profile free webmail users being spied on for more than a year.

Spear-Phishing Campaigns

Pawn Storm tries to snare targets using spear-phishing emails that have a malicious attachment or emails that link to an exploit URL. The spear-phishing emails are usually about a recent event covered in the news that is likely to be of interest to the targets. Pawn Storm often uses the exact same headlines from recent news reports seen on media sites like CNN, Al Jazeera, Huffington Post, Military Times and many others.

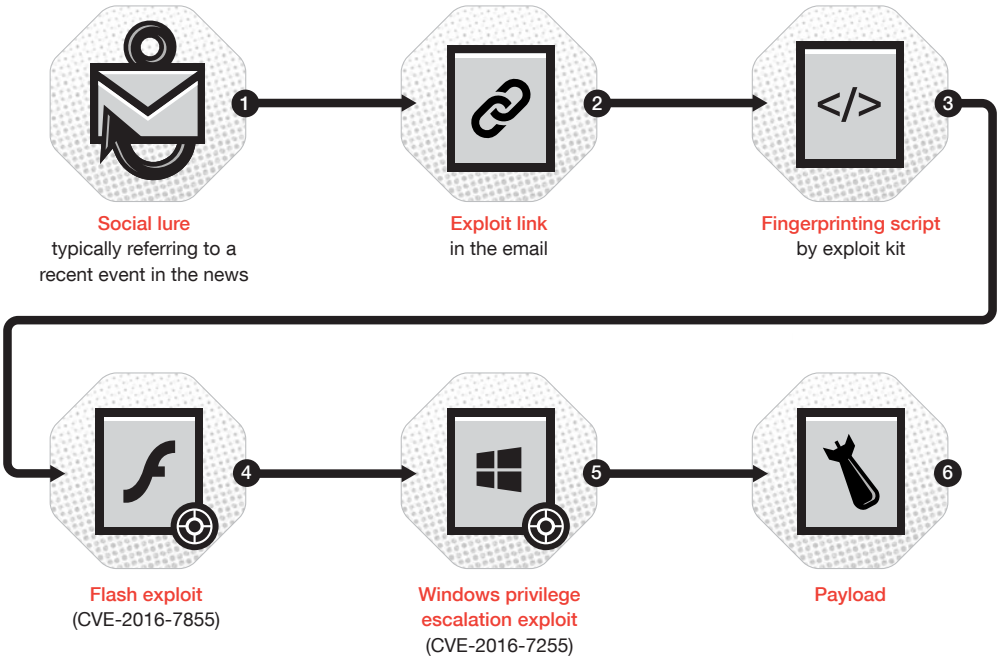


Figure 10. Typical infection chain of Pawn Storm's spear-phishing campaigns

In 2015 and 2016 Trend Micro blocked dozens of these spear-phishing campaigns against high profile customers. Below we list some of the spear-phishing emails that contained a link to the private exploit kit of Pawn Storm, as well as the date and email subject line used.

Date	Subject line
02/03/15	Pro-Russian rebels launch new offensive
03/18/15	NATO's role in conventional arms control
03/25/15	Open Skies Consultative Commission
03/26/15	News: Exercise Ramstein Dust I 2015 is underway in Italy
04/01/15	News: Yemen air strikes kill 23 in factory: residents
04/01/15	National Armaments Directors
04/01/15	Heavy clashes on Saudi-Yemeni border
04/06/15	North Korea declares no-sail zone, missile launch seen as possible - reports

Date	Subject line
04/06/15	What does Russia's President Putin really want?
04/06/15	Ukraine Today: Russian-backed militants appeal to Merkel
04/06/15	Ambassador of Ukraine to Jordan Dr. SergiyPasko held talks with Director of the European Department of the MFAE of Jordan Mr. Daifallah al-Fayez
04/08/15	Petro Poroshenko congratulated Muhammadu Buhari on his election as President of the Federal Republic of Nigeria
04/15/15	News: Obama, in 'therapeutic' meetings with U.S. Jewish leaders, stresses how much he cares
04/21/15	China, Japan and South Korea hold renewed talks
04/22/15	News: Foreign Ministry denies any suspected incidence of corruption in Tunisia's embassy in Amman
04/30/15	News: Tragedy in Nepal
05/05/15	News: Chimerica in Decline?
05/07/15	Diplomatic Access: The United States
05/12/15	News: Can China and the EU Cooperate on International Security?
05/13/15	News:Kerry: Now is 'Critical Moment' for Ukraine Conflict
05/15/15	Russian soldiers quit over Ukraine
05/20/15	Foreign Minister Szijjarto: NATO must respond to new threats
06/17/15	Ambassadors RSG Wolfsbos bezoeken Europees Parlement
06/19/15	Pew Survey: Irredentism Alive and Well in Russia
07/03/15	For Your Information:Latest from OSCE Special Monitoring Mission (SMM) to Ukraine
07/08/15	For Your Information:Latest from OSCE Special Monitoring Mission(SMM) to Ukraine
07/09/15	For Your Information:ANNUAL MEETING & EXPOSITION 12-14 October 2015
07/09/15	Iran nuclear deal: Snapping back sanctions
07/10/15	CNN Politics:What the Iran deal is really about
07/23/15	NATO Won't Establish Permanent Military Bases In Poland Amid Russia Tension, US Diplomat Says
08/27/15	Russia to increase wheat supplies to Egypt, says Putin
09/08/15	Iraq Puts New F-16s Into Action Against ISIS Jihadists
09/09/15	Bulgaria Bars Syria-Bound Russian Planes as NATO Fears Grow
09/16/15	Russia gives Assad firepower, spurring US strategy adjustment
09/17/15	Burkina Faso: an attempted coup?
09/18/15	Croatia closes road border crossings with Serbia after migrant influx

Date	Subject line
09/21/15	US, Russian Defense Heads Talk about Syrian Military Buildup
09/21/15	Tsipras returns as PM in decisive Greek election
09/22/15	Foreign Information Policy
09/22/15	THE FIGHT AGAINST ISIS
09/22/15	Despite Attention to Islamic State, Al-Qaida May Be Bigger Threat
09/23/15	US military reports 75 US-trained rebels return to Syria
09/24/15	Assad is Moscow's pawn in regional power stakes
09/24/15	Russia Warns of Response to Reported US Nuke Buildup in Turkey
10/01/15	Russia rejects claims its 'anti-sisl' airstrikes hitcivilians and other rebels
10/05/15	Israel launches airstrikes on targets in Gaza
10/12/15	Suicide car bomb targets NATO troop convoy in Kabul
10/12/15	Syrian troops make gains as Putin defends air strikes

Table 3. Spear-phishing campaigns by Pawn Storm in 2015, data from Trend Micro's Smart Protecting Network

The subject lines clearly indicate that Pawn Storm uses recent newsworthy events to encourage victims to click. Though these are targeted attacks, some of the campaigns are relatively noisy and have been frequently deployed from 2015 to 2016. Most of the attacks were not widely reported in media, but some did make it to the news.

In 2016, awareness grew due the amount of research that was published by Trend Micro and other Internet security vendors. For example in September 2016 several major German newspapers published stories of German politicians that were being attacked by Pawn Storm in August 2016. We can confirm that Trend Micro saw spear-phishing emails sent by Pawn Storm using German political themes as social engineering lures. However these emails were part of a much bigger campaign with targets in many other countries as well. The spear-phishing campaigns as reported in the German media were actually not that uncommon, but almost business as usual for the Pawn Storm actors. Still, it shows that in 2016 the actors showed a clear interest in compromising political organizations.

Though some of the spear-phishing emails are relatively noisy, Pawn Storm is careful with how they infect their targets. First of all, the exploit URLs are specific for every victim—each has a parameter that is unique to the particular target. In case a target clicks on an exploit URL, he will first get fingerprinted with invasive JavaScript code that is not malicious by itself. The JavaScript will upload information like the Operation System, language settings, browser plugins, and time zone of the target's computer to the exploit server. Depending on the fingerprinting results, the exploit server might give back an old exploit, a

zero-day, or a social engineering lure[16]. In a lot of cases nothing will happen, apart from a redirection to a benign news site that has an article related to the social engineering lure of the spear-phishing email. The use of a zero-day will also depend on how valuable that zero-day still is to Pawn Storm. Once the zero-day gets discovered and a fix is underway, its value in the attack portfolio will be devalued.

In 2016 we witnessed that during the interval of a Windows privilege escalation vulnerability being disclosed and then patched, Pawn Storm ramped up its operations and targeted a broader range of governmental personnel. The group used the just-patched Flash zero-day and the still open Windows privilege escalation vulnerability[17].

Even when a target does get infected with malware, he will first get relatively simple first stage malware installed. This gives Pawn Storm another chance to learn whether a target is worth a deeper probe. If the target is interesting enough, the actor will install second stage components like X-Agent and X-Tunnel. After this, Pawn Storm might try to penetrate deeper into the network infrastructure, so that it can control more nodes in the victim's network.

In 2016, Pawn Storm started to use RTF and other Office documents embedded with a Flash file. The Flash file will upload information on the targets' system to a remote server. We have witnessed that the remote server may respond with a chain of exploits, zero-days and privilege escalation that will infect the target's computer. This kind of infection chain was first described by Palo Alto Network researchers and dubbed Dealers Choice[18].

Preferred Attacks, Resources, and Tools

Watering Hole Attacks

Pawn Storm has compromised websites that targets are likely to visit. For this kind of attack, the actors have to wait and see who will visit the compromised sites. On these compromised sites, Pawn Storm can choose to inject scripts that will serve their objectives. We have seen instances where Pawn Storm injected the so-called Browser Exploitation Framework (BeEF)[19] exploit on legitimate websites. In other cases, links were inserted that would lead to Pawn Storm's private exploit kit.

Like the name already suggests BeEF works from the browser to attack Internet users. BeEF is used by legitimate penetration testers and it is very invasive. The framework includes many modules, including tools for reconnaissance, social engineering and active exploitation of vulnerabilities.

BeEF is particularly useful to an attacker when the target doesn't close inactive tabs in his Internet browser. When an Internet user opens a browser tab and visits a website that has been compromised to link to a BeEF exploit URL, the attacker has ample time to do reconnaissance and try out different attacks until the browser tab gets closed. These attacks may include social engineering attacks, grabbing passwords, and exploiting vulnerabilities.

We have seen that the website of a Ukrainian defense company was compromised to link to a BeEF exploit on a remote server. Visitors of the defense company's website are likely to be interesting targets to Pawn Storm, and might have been exposed to various attacks. An injection of a BeEF exploit happened to the websites of some Ministries of Foreign Affairs in Europe and Africa as well.

Earlier in 2014, Pawn Storm compromised Polish government sites and the website of the Power Exchange in Poland. Visitors to the websites were exposed to Pawn Storm's private exploit kit.

And as we previously mentioned, in June 2016 Pawn Storm compromised the website of the DCCC. Anyone donating money via dccc.org would be redirected to a Pawn Storm-controlled site. Pawn Storm possibly intended to compromise donors of the Democratic Party in the US and to spy on them. However we have not been able to confirm the exact infection chain.

Zero-Days

Pawn Storm is known to have used several zero-days[20]. For example, at the end of October 2016 Pawn Storm was identified as using a Flash zero-day together with a privilege escalation in Windows. Soon after the Flash vulnerability (CVE-2016-7855) was patched, Pawn Storm started to make the most out of these partially patched zero-days by exposing more targets to them. On October 28 2016 a relatively noisy campaign was launched that sent several RTF documents to targets.

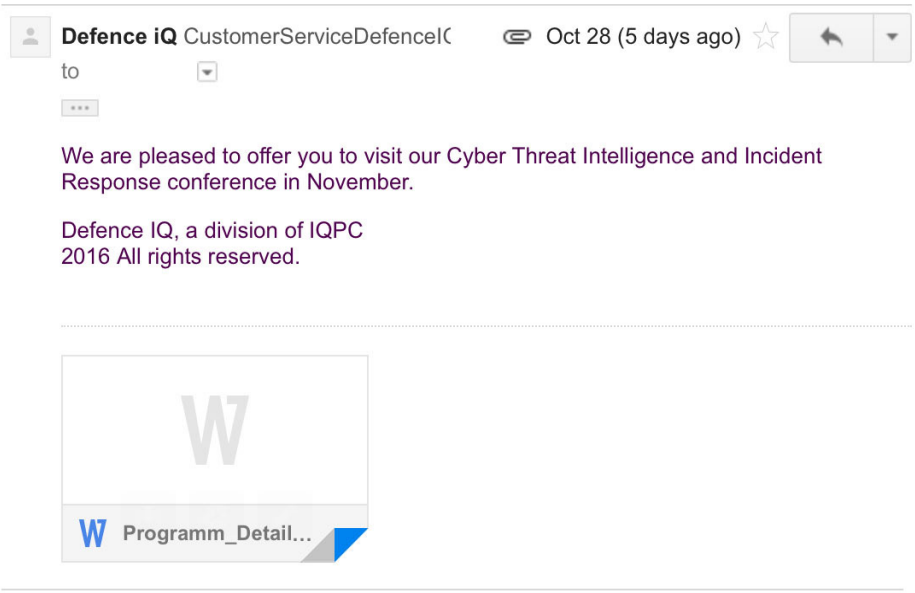


Figure 11. A Pawn Storm spear-phishing email with an RTF document

The RTF document has a Flash file embedded in it that is a simple downloader. We saw that it first downloaded an encrypted Flash exploit (CVE-2016-7855) from a remote server. Then it downloaded a second file that crashed Microsoft Word. In other reported cases the second file was a first stage payload of Pawn Storm.

In July 2015 Trend Micro discovered a Java zero-day that was exploited together with a privilege escalation that evades the click to play protection in Java.

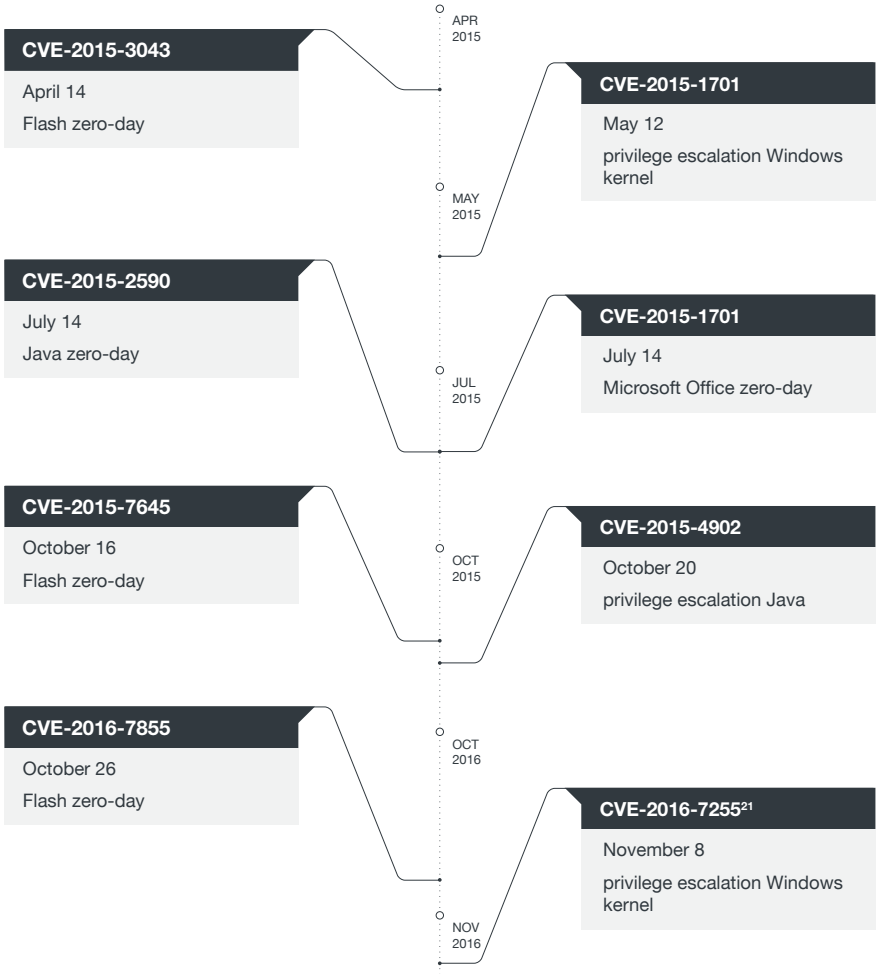


Figure 12. Zero-days that are believed to have been used by Pawn Storm exclusively beforethey were patched

Apart from these zero-days, Pawn Storm was also quick to use other vulnerabilities that were disclosed in the leaks of Hacking Team.

Second Stage C&C Servers

The uptick in Pawn Storm's activity over the recent years becomes very clear in a graph which shows active second stage C&C servers from 2015 until today.

We were able to keep track of the live second stage C&C servers from late 2013 until today. At the end of 2013 there were about five live X-Agent C&C servers. In early October 2016, we counted 26 live X-Agent C&C servers. This is a strong indication that Pawn Storm has been very active in 2016.

Another local peak was in the fall of 2014, possibly because around that time Trend Micro's first paper on Pawn Storm was published and the actor group made changes to their infrastructure.

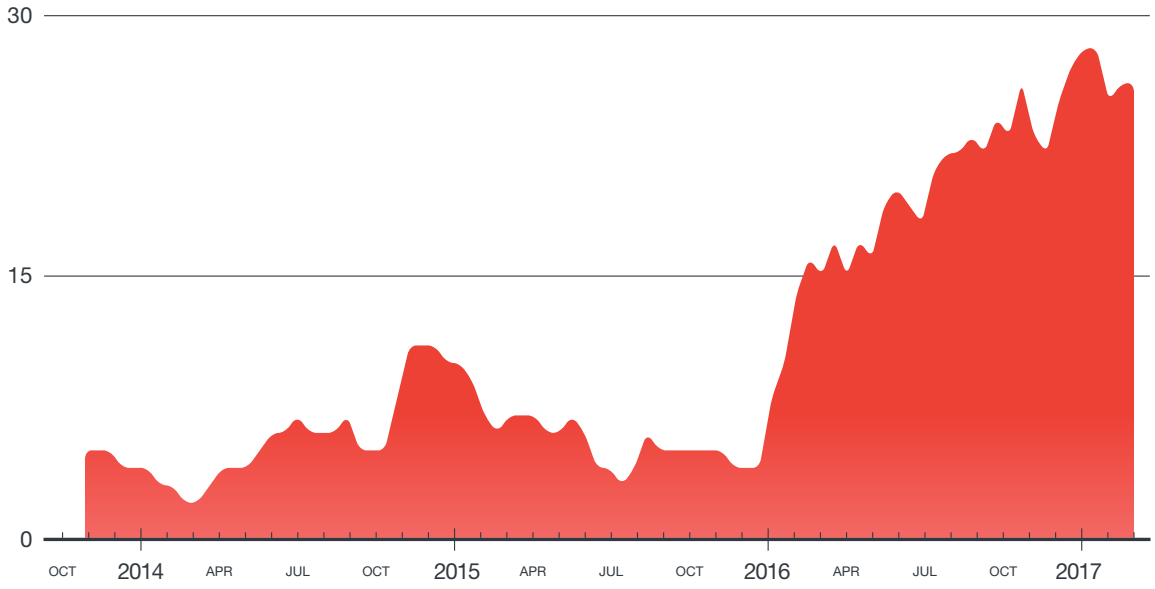


Figure 13. Tracking the number of live X-Agents C&Cs from Oct 2013 to Feb 2017

Around the Christmas holidays of 2016, the number of live X-Agents C&Cs slightly increased to 27. In January 2017 the number peaked at 28 live X-Agent IP addresses. Pawn Storm did not take a long break during the 2016 holidays. Right after Christmas, on December 26 2016, we saw Pawn Storm recommence their spear-phishing campaign. In January 2017, the usual credential phishing also continued.

Facilitators

Pawn Storm has a clear preference for certain webhosting providers and registrars. This preference is sometimes so specific that newly set up domains can be spotted before they are even used in attacks. In recent months, however, Pawn Storm's use of IP ranges is getting more diverse and parts of their activity have become more difficult to track.

Generally speaking, Pawn Storm uses the Internet infrastructure in well-connected countries like the US, UK, France, Netherlands, Latvia, Romania and Germany. In these countries, the national intelligence services could probably easily and legally intercept connections to Command and Control servers, sources of (spear) phishing emails, and Pawn Storm's exploit sites that are set up in their country. Encryption and TLS in both web traffic and email traffic will limit the usefulness of these legal intercepts, though.

For example, for sending credential phishing emails Pawn Storm probably doesn't have to worry about authorities unless the authorities have access to the servers that are sending the emails. In the table below we illustrate the infrastructure that was used by Pawn Storm to send out Yahoo credential phishing emails in 2015. As far as we are aware, for all of 2015, Pawn Storm only used one IP address in Germany and one in Netherlands to send out the phishing emails.

Date	Sender IP	Server Name	Backend IP	Server Name
Jan-15	80.255.3.94	ubuntu	46.166.162.90	Henry-PC
Feb-15	80.255.3.94	ubuntu	46.166.162.90	Henry-PC
Feb-15	193.169.244.35	security.service-facebook.com	46.166.162.90	Henry-PC
Mar-15	80.255.3.94	ubuntu	46.166.162.90	Henry-PC
Mar-15	193.169.244.35	security.service-facebook.com	46.166.162.90	Henry-PC
Apr-15	193.169.244.35	security.service-facebook.com	46.166.162.90	Henry-PC
Apr-15	193.169.244.35	security.service-facebook.com	46.183.217.74	Henry-PC
May-15	193.169.244.35	security.service-facebook.com	46.183.217.74	Henry-PC
Jun-15	80.255.3.94	set121.com	46.183.217.74	Henry-PC
Jul-15	80.255.3.94	set121.com	46.183.217.74	Henry-PC
Aug-15	193.169.244.35	security.service-facebook.com	46.183.217.74	Henry-PC
Sep-15	80.255.3.94	set121.com	46.183.217.74	Henry-PC
Oct-15	193.169.244.35	security.service-facebook.com	46.183.217.74	Henry-PC
Nov-15	193.169.244.35	security.service-facebook.com	46.183.217.74	Henry-PC
Nov-15	193.169.244.35	security.service-facebook.com	185.82.202.102	WIN-17MK2DLAHLN
Nov-15	80.255.3.94	exua.email	N/A	N/A
Nov-15	193.169.244.35	security.service-facebook.com	87.121.52.145	Hans-PC
Dec-15	193.169.244.35	security.service-facebook.com	87.121.52.145	Hans-PC
Dec-15	193.169.244.35	security.service-facebook.com	185.82.202.102	WIN-17MK2DLAHLN

Table 4. Infrastructure used in 2015 by Pawn Storm to send credential phishing emails to high profile Yahoo users

In 2016 Pawn Storm started to use legitimate email providers like GMX and Yandex to send out credential phishing emails from VPN servers like IPVanish.

Actual data communication to C&C servers like X-Agent will be encrypted and this means that exfiltrated data cannot be read unless a decryption algorithm is available. Pawn Storm clearly doesn't care that intelligence services might have some visibility on the identities of the victimized targets.

This becomes even more apparent when we realize that a lot of the X-Agent C&Cs are live for several months. Averaged over 3 years of data, X-Agent C&Cs are live for 6 months. Ten of the X-Agent C&Cs were live for more than 12 months. This shows that the Pawn Storm is somewhat brazen: the actors don't really care if they get caught at some point. You could consider this bad operational security, however it also indicates the difficulties targets face when defending against the Pawn Storm actors. In a lot of the attacks the actors get what they were after anyway.

The graph below shows the distribution of second stage X-Agent C&C servers to each country from November 2013 until February 2017. It clearly illustrates the distribution of live C&C servers averaged over a 3 year period.

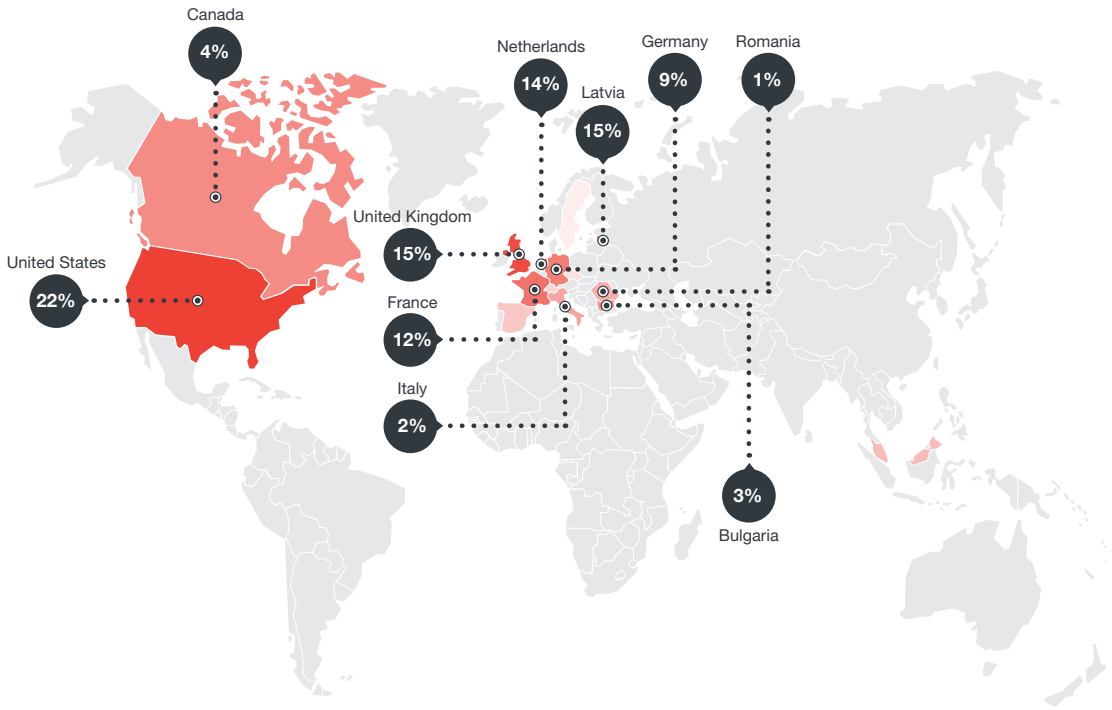


Figure 14. Distribution of live X-Agent C&C servers averaged over a 3 year period

Operational Security

Operational security is defined as the precautions that actors take to hide their activities and whereabouts. The operational security of Pawn Storm is quite remarkable, since for many of its operations it has become apparent that hiding activities is not always a high priority for the Pawn Storm actors. However, actions of Pawn Storm cannot easily be attributed to nicknames or profiles in the underground. For many cybercriminal groups at least some nicknames from the underground are known, but not so with this group. The identities of the individual Pawn Storm actors seem to be protected very well. Pawn Storm has a clear preference for some hosting providers, DNS service providers, and domain registrars. By monitoring these service providers, it can be relatively easy for a researcher to spot new infrastructure that is being set up. In this way, a lot of Pawn Storm's infrastructure can be discovered early—sometimes even before the attacks have actually started.

There is another side of this apparent lack of operational security though. Pawn Storm is also using anonymous registration of domains, and in certain cases they choose very different providers. Attacks using this infrastructure might easily get overlooked and not attributed to Pawn Storm.

Moreover, the preferred service providers of Pawn Storm give the actors good anonymity, one reason being these providers usually accept Bitcoin as payment. Pawn Storm makes good use of webhosting providers in Western countries that offer privacy to their customers. We don't know for sure whether these hosting companies are knowingly providing services to cyber criminals and cyber spies, perhaps at premium rates. However some of the webhosting companies have had ties with so called Bulletproof hosting providers in the past. We actually described an example of a hosting provider in the Netherlands in a 2016 article[22]. We witnessed that Pawn Storm makes extensive use of VPN servers to connect to free webmail providers and then send out spear-phishing emails to their targets. Some of the C&C servers may just relay traffic to intermediate proxies and thus relay stolen data back to the actual backend servers over more than one hop. Just a couple of proxy nodes will greatly enhance operational security and anonymity of the actors.

Even when the infrastructure of Pawn Storm gets discovered quickly, vast amounts of data might have already been exfiltrated to a foreign computer server before the target is aware something is happening. There are several examples of infections and compromises that were discovered after months, and even after more than a year in some cases.

The vast majority of the campaigns Pawn Storm is doing would interest intelligence services around the world. Investigations by normal police will usually lead nowhere as the problem of espionage[23] can only be addressed at higher political levels and not by criminal investigations. Communications between different law enforcement agencies are not always optimal within one country and between different countries. This can imply that agency X in a country may know about an attack by Pawn Storm in its country or another country, but is unable to inform the target in a timely manner. This further adds to the success of actors like Pawn Storm.

It is not unthinkable that the Pawn Storm actors actually appreciate it when researchers dissect and write about their operations (after they have achieved their goal anyway). These articles are likely to be picked up by mass media, which the actors may consider as free publicity of their capabilities and the media reports might also be damaging to the affected target organizations. Normal cybercriminals often don't like media attention and even suspend their activities temporarily when their actions are discovered and written about. Pawn Storm doesn't slow down at all. On the contrary: a lot has been written about Pawn Storm since fall of 2014, and their activities have only grown, both in aggressiveness and number.

Conclusion and Defending Against Pawn Storm

This closer look at the activities, operational capacity, and tactics of Pawn Storm gives a comprehensive picture of the group's real motives and capabilities. With a clear understanding of the trends that Pawn Storm is following, along with their history and past operations, hopefully potential victims and targets can properly address this threat. This last section is dedicated to defending against Pawn Storm.

Protecting yourself against an attacker like Pawn Storm is a challenge. They have resources that allow them to run lengthy campaigns over years, and seem to be single-minded in their pursuit of their targets. We've seen how the group's credential phishing tactics work to ensnare even the most savvy webmail users, and how sophisticated their attacks look. Pawn Storm has used several zero-days in 2015 and 2016. They also have well-established tactics, from using tabnabbing to compromising DNS settings, creating watering holes and advanced social engineering. And they have no trouble finding new ways to abuse technology.

Pawn Storm attacks from many different sides, and dedicate more of their resources when they identify a worthwhile target. Successfully repelling numerous attacks is not a guarantee; only one has to succeed for the attackers to achieve their goal.

However, there are some things you can do to raise the level of your defenses:

1. Minimize your attack surface—systems that do not need to be exposed to the open Internet shouldn't be.

2. Require remote workers to use the corporate VPN to access your systems.

3. Minimize the number of domain names you maintain and centralize email servers.

4. Prevent DNS hijacking of your domains. Work with reputable registrars only, or those that allow for two-factor authentication of your DNS administrator account. Lock your domain at the registrar to further raise the bar for unauthorized changes to your domains. For example you could choose to

let your registrar call back your authorized DNS administrator to double check whether changes to DNS zones really have to be made.

5. Enforce two-factor authentication for corporate webmail, or a better option would be to require authentication by means of a physical (USB) security key.

6. Educate employees on securing their private free webmail and social media accounts too, and don't let them use those accounts for work purposes.

7. When your employees travel overseas or attend conferences, let them take a clean loan computer with them. Wipe the data from the computer and do a fresh OS install after the trip.

8. Outsourced services can be compromised too, use only reputable third-party services.

9. Educate workers about email system and/or email account best practices: specifically, don't store sensitive information in email boxes without encryption and don't send sensitive information by email without encryption.

10. Let a reputable company do penetration testing of your network regularly. Include social engineering in these tests.

11. Keep software updated and patched.

References

1. TrendLabs. (22 July 2004). *Trend Micro Threat Encyclopedia*. “TROJ_SCONATO.A”. Last accessed 08 Match 2017. http://www.trendmicro.com/vinfo/us/threat-encyclopedia/archive/malware/troj_sconato.a.

2. L.Kharouni, F. Hacquebord, N.Huq, J. Gogolinski, F.Mercês, A.Remorin, D. Otis. (22 October 2014). *Trend Micro*. “Operation Pawn Storm: Using Decoys to Evade Detection.” Last accessed on 12 March 2017. http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-pawn-storm.pdf.

3. TrendLabs. (16 January 2016). *Trend Micro*. “Operation Pawn Storm: Fast Facts and the Latest Developments.” Last accessed on 20 February 2017. https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-pawn-storm-fast-facts.

4. TrendLabs. (10 March 2017). *Trend Micro*. “Cyber propaganda 101”. Last accessed 13 March 2017. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/cyber-propaganda-101.

5. Eset researchers. (20 October 2016). *ESET*. “Dissection of Sednit Espionage Group”. Last accessed 17 March 2017. https://www.eset.com/int/about/newsroom/research/dissection-of-sednit-espionage-group/.

6. FireEye Threat Intelligence (27 October 2014). *FireEye*. “APT28: A Window into Russia’s Cyber Espionage Operations?“ Last accessed 16 March 2017. https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf.

7. R. Benchea, C. Vatamanu, A. Maximciuc, V. Luncaşu. *Bit Defender*. “APT28 Under the Scope: A Journey into Exfiltrating Intelligence and Government Information.” Last accessed 13 March 2017. http://download.bitdefender.com/resources/media/materials/white-papers/en/Bitdefender_In-depth_analysis_of_APT28%E2%80%93The_Political_Cyber-Espionage.pdf.

8. Security Intelligence Microsoft. (16 November 2015). *TechNet Microsoft*. “Microsoft Security Intelligence Report: Strontium”. Last accessed 15 March 2017. https://blogs.technet.microsoft.com/mmpc/2015/11/16/microsoft-security-intelligence-report-strontium.

9. ThreatConnect Research Team. (12 August 2016). *ThreatConnect*. “Does a Bear Leak in the Woods?” Last accessed 3 March 2017. https://www.threatconnect.com/blog/does-a-bear-leak-in-the-woods/.

10. R. Buschmann, L. Eberle, C. Henrichs and G. Pfeil. (15 January 2017). *Der Spiegel*. “Inside the Desperate Battle against Sports Doping”. Last accessed 16 March 2017. http://www.spiegel.de/international/world/sports-doping-and-the-difficult-fight-to-prevent-it-a-1129918.html.

11. Feike Hacquebord. (11 May 2016). *Trend Micro*. “Pawn Storm Targets German Christian Democratic Union”. Last accessed 13 March 2017. http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-targets-german-christian-democratic-union/.

12. Feike Hacquebord. (7 March 2016). *Trend Micro*. “Pawn Storm Campaign Adds Turkey To Its List of Targets”. Last accessed 10 March 2017. http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-adds-turkey-list-targets/.

13. Feike Hacquebord. (18 August 2015). *Trend Micro*. “Pawn Storm’s Domestic Spying Campaign Revealed; Ukraine and US Top Global Targets”. Last accessed 13 March 2017. http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storms-domestic-spying-campaign-revealed-ukraine-and-us-top-global-targets/.

14. AzaRaskin. *Aza Rask.in*. “Tabnabbing: A New Type of Phishing Attack.” Last accessed on, 7 March 2017. http://www.azarask.in/blog/post/a-new-type-of-phishing-attack/.

15. Feike Hacquebord. (24 October 2014). *Trend Micro*. “Operation Pawn Storm: Putting Outlook Web Access Users at Risk” Last accessed 15 Febuary 2017. http://blog.trendmicro.com/trendlabs-security-intelligence/operation-pawn-storm-putting-outlook-web-access-users-at-risk/.

16. Feike Hacquebord. (16 April 2015). *Trend Micro*. "Operation Pawn Storm Ramps Up its Activities; Targets NATO, White House" Last accessed 16 March 2017. http://blog.trendmicro.com/trendlabs-security-intelligence/operation-pawn-storm-ramps-up-its-activities-targets-nato-white-house/.

17. Feike Hacquebord, Stephen Hilt. (9 November 2016). *Trend Micro*. "Pawn Storm Ramps Up Spear-phishing Before Zero-Days Get Patched" Last accessed 17 March 2017. http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-ramps-up-spear-phishing-before-zero-days-get-patched/.

18. Robert Falcone, Bryan Lee. (17 October 2016). Research Center Paolo Alto Networks. "'Dealers Choice' is Sofacy's Flash Player Exploit Platform". Last accessed 2 March 2017. http://researchcenter.paloaltonetworks.com/2016/10/unit42-dealerschoice-sofacys-flash-player-exploit-platform/.

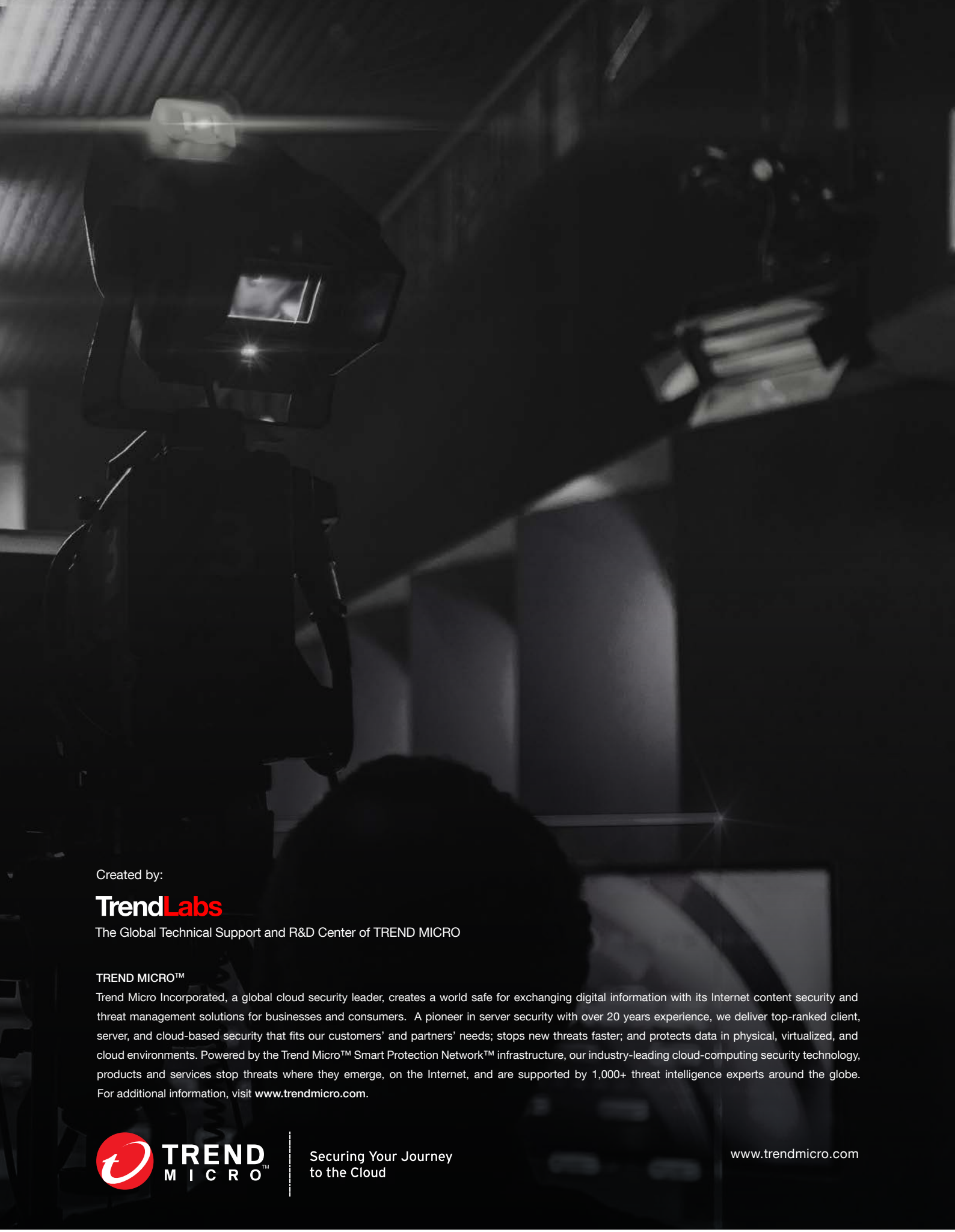
19. The Browser Exploitation Framework Project. Last accessed 8 March 2017. http://beefproject.com/.

20. Brooks Li, Feike Hacquebord. (11 July 2015). *Trend Micro*. "Pawn Storm Update: Trend Micro Discovers New Java Zero-Day Exploit" Last accessed 16 March 2017. http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-update-trend-micro-discovers-new-java-zero-day-exploit/.

21. Jack Tang. (2 December 2016). *Trend Micro*. "One Bit To Rule A System: Analyzing CVE-2016-7255 Exploit In The Wild" Last accessed 20 February 2017. http://blog.trendmicro.com/trendlabs-security-intelligence/one-bit-rule-system-analyzing-cve-2016-7255-exploit-wild/.

22. Feike Hacquebord. (21 April 2016). *Trend Micro*. "Looking Into a Cyber-Attack Facilitator in the Netherlands." Last accessed 15 March 2017. http://blog.trendmicro.com/trendlabs-security-intelligence/looking-into-a-cyber-attack-facilitator-in-the-netherlands/.

23. Roman Dobrokhotov. (8 November 2016). *Aljazeera*. "Under surveillance in Russia." Last accessed12 March 2017. http://www.aljazeera.com/indepth/opinion/2016/11/surveillance-russia-161107133103258.html.



Created by:

TrendLabs

The Global Technical Support and R&D Center of TREND MICRO

TREND MICRO™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver top-ranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit **www.trendmicro.com**.

TREND MICRO™

Securing Your Journey to the Cloud

www.trendmicro.com