

Operation Pawn Storm

Using Decoys to Evade Detection

Loucif Kharouni
Feike Hacquebord
Numaan Huq
Jim Gogolinski
Fernando Mercês
Alfred Remorin
Douglas Otis
Forward-Looking Threat Research Team



CONTENTS

Introduction.....	1
Ties That Bind the Operation Pawn Storm Attacks Together.....	2
SEDNIT.....	2
Attack Timeline	2
Attack Details.....	4
Attack Evolution.....	5
Next-Level Phishing Targets.....	11
Case 1: Ministry of Defense, Hungary.....	11
Case 2: OSCE, Austria	13
Case 3: SAIC, United States	13
Case 4: Academi.....	13
Other Webmail Services.....	14
Conclusion.....	16
References	17

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.

INTRODUCTION

Operation Pawn Storm refers to economic and political espionage attacks instigated by a group of threat actors primarily targeting military, embassy, and defense contractor personnel from the United States and its allies. Opposing factions to and dissidents of the Russian government, international media, and even the national security department of a U.S. ally were also targeted. The threat actors used three attack vectors—spear-phishing emails with malicious attachments, an advanced network of phishing websites, and exploits injected into legitimate conference and media websites. They used a nonmalicious JavaScript to victimize Microsoft™ Outlook® Web Access (OWA) users from carefully selected target organizations. The OWA phishing attacks proved extremely effective and could be

particularly dangerous to any organization that allows employees to use OWA.

An in-depth look at six multistage attacks revealed one thing in common—the use of SEDNIT/Sofacy malware [1], [2]. The use of such multistage downloaders provided attackers additional protection against detection. We believe the threat actors aimed to confuse their targets' IT administrators by making it hard for them to string attack components together, thus evading detection.

This research paper details when certain attacks occurred, what tools were used in attempts to get in to target networks, and target profiles to form a general picture of Operation Pawn Storm.

TIES THAT BIND THE OPERATION PAWN STORM ATTACKS TOGETHER

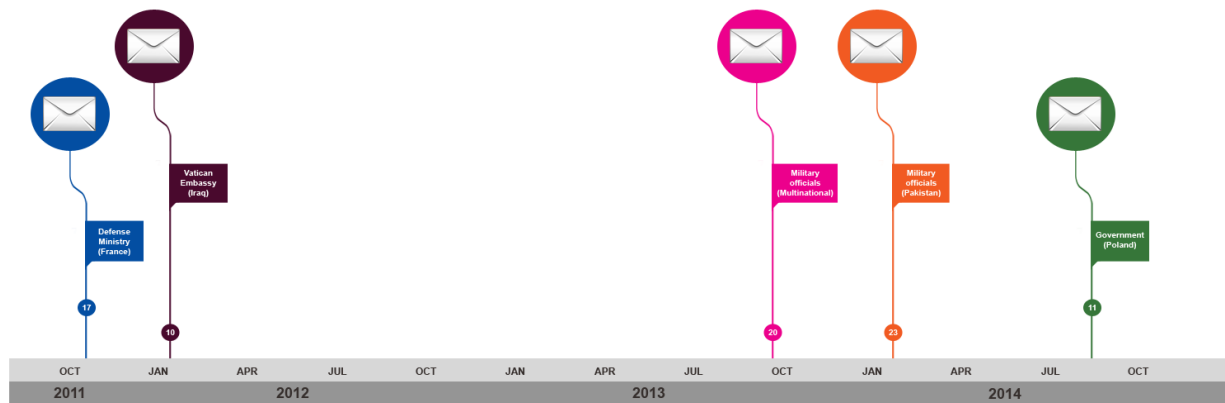
SEDNIT

SEDNIT malware are mostly backdoors [3], [4] and information stealers [5] that log affected users' keystrokes, steal system information, and send stolen information to remote command-and-control (C&C) servers.

Analyses of the SEDNIT infectors that arrived as email attachments in the attacks featured in this paper revealed six distinct chains [see diagram on page 3].

Attack Timeline

The investigation focused on a group of attacks that has been dubbed "Operation Pawn Storm" [6] due to the attackers' use of two or more connected tools/tactics to attack a specific target similar to the chess strategy it was named after. This paper illustrates how the Pawn Storm attacks were carried out with the aid of five spear-phishing emails, which used contextually relevant subjects to get specific targets from different countries to open weaponized attachments designed to compromise their systems.



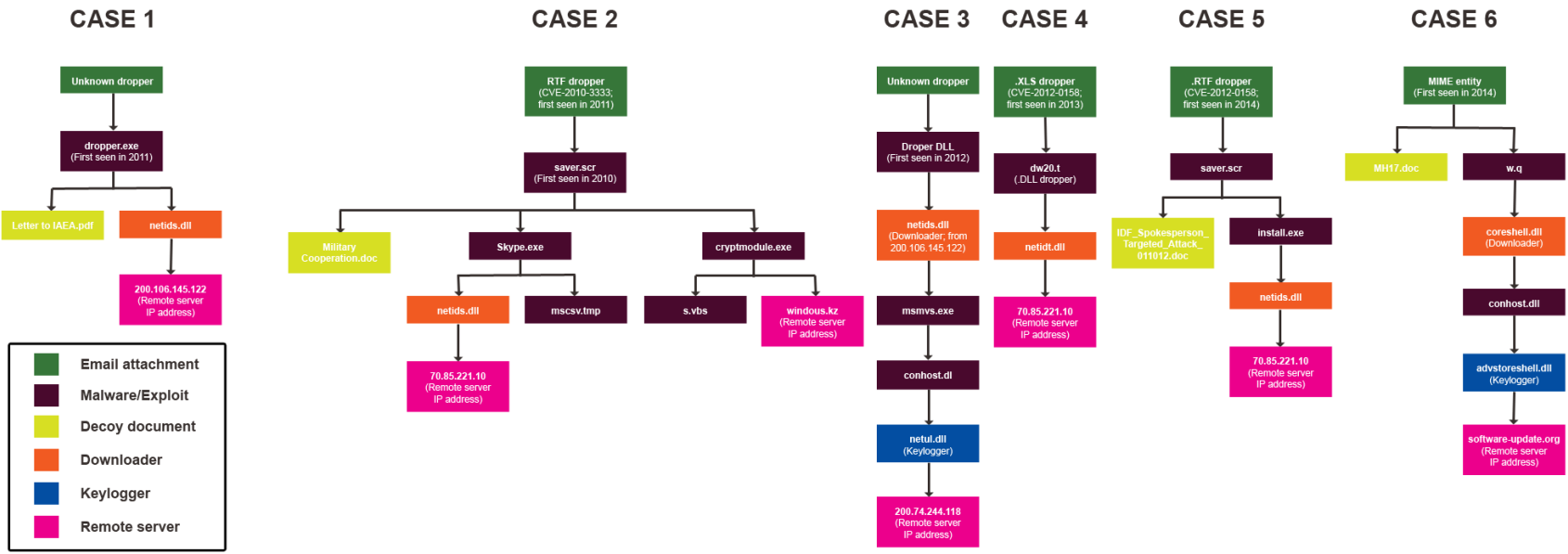
Timeline of spear-phishing emails sent to specific targets

The attackers sent emails to potential victims, including military, embassy, and defense contractor personnel. The following emails were among those that were found related to this operation:

- An email sent to a potential victim from the Ministry of Defense in France had an exploit for CVE-2010-3333 [7] disguised as a document named

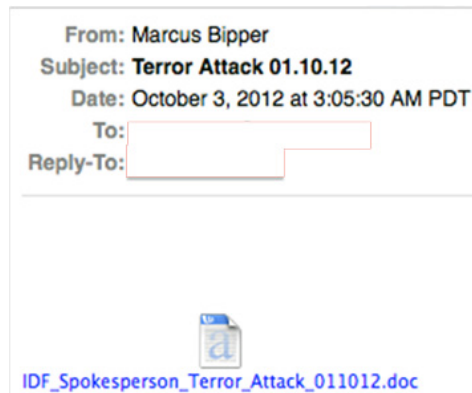
"International Military.rtf." Trend Micro received a sample of this on October 17, 2011 and has been detecting it as TROJ_ARTIEF.AP [8] since then.

- An email sent to a potential victim working from the Vatican Embassy in Iraq used reports of a bombing incident [9] that occurred on January 9, 2012 as social engineering lure.

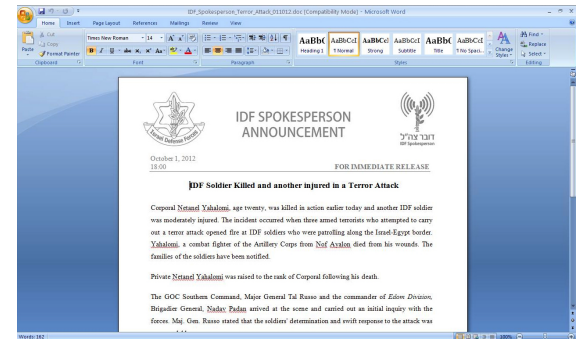


SEDNIT infectors attached to targeted attack campaign emails

Sent a day after the incident, the email had a Microsoft Word® file attachment named “IDF_Spokesperson_Terror_Attack_011012.doc,” which exploited CVE-2012-0158 [10].

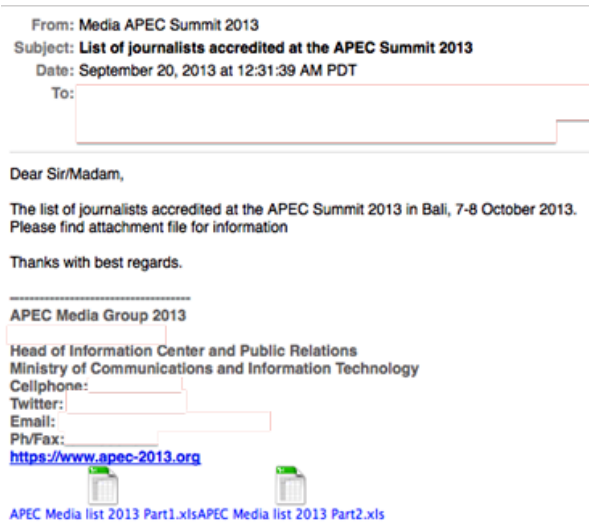


Sample email sent to recipients from the Vatican Embassy in Iraq



Exploit for CVE-2012-0158 disguised as a Word (.DOC) file

- An email sent on September 20, 2013 to military officials from several countries used the then-upcoming “Asia-Pacific Economic Cooperation (APEC) Indonesia 2013” conference as bait. The email had two Microsoft Excel® file attachments named “APEC Media list 2013 Part1.xls,” which exploited CVE-2012-0158, and “APEC Media list 2013 Part2.xls,” which was nonmalicious.



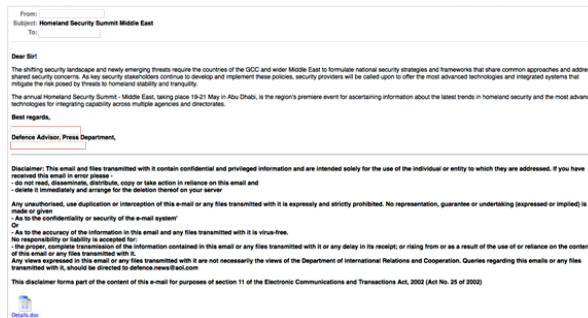
Sample email sent to military officials across countries using the “APEC Indonesia 2013” conference as bait

No.	First Name	Last Name	Gender	Email	Nationality	Identity Number	Name of Media
1	Levent	Uslu	Male	luyucan.com	Afghanistan		Middle east press
2	Alex		Male	@fairfaxmedia.com.au	Australia		Fairfax Media
3	Alexander		Male	@seven.com.au	Australia		Seven Network Australia
4	Nobuyuki		Female	@nbc.com	Australia		NBC Australia Network
5	David		Male	@gmail.com	Australia		ABC/Australian Broadcasting Corporation
6	Ronald		Female	@blomberg.net	Australia		Blomberg LP
7	Roxanne		Female	@gmail.com	Australia		The Asia Stream
8	George		Male	@vivoon.com	Australia		Phoenix Satellite Television Co Ltd
9	George		Male	@gmail.com	Australia		ABC/Australian Broadcasting Corporation
10	Norm		Female	@rtm.com.au	Australia		Rine Network
11	Jennifer		Female	@2gb.com	Australia		Madque Radio Network
12	Paul		Male	@cnn.com	Australia		CNN International
13	Peter		Male	@theaustralian.com.au	Australia		The Australian
14	Michael		Male	@theage.com.au	Australia		Sydney Morning Herald and The Age
15	Daniel		Male	@gmail.com	Australia		CCTV News
16	KARL		Male	@frp.com	Australia		The Australian
17	Simon		Male	@news.com.au	Australia		AGENCE FRANCE PRESSE (AFP)
18	Michael		Male	@abc.com.au	Australia		News Corporation
19	Richard		Male	@abc.com.au	Australia		Fairfax Radio/2UE
20	James		Male	@abc.com.au	Australia		SBS TV
21							ABC

Exploit for CVE-2012-0158 disguised as an Excel (.XLS) file (APEC Media list 2013 Part1.xls)

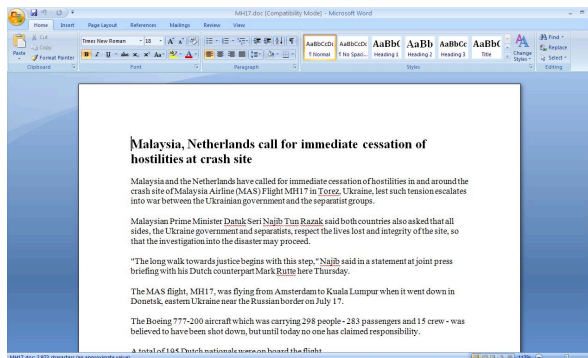
- An email sent to Pakistani military officials on January 23, 2014 used the “Homeland Security Summit Middle East” [11] conference as bait. It had a Word file attachment named “Details.

doc,” which exploited CVE-2012-0158.



Sample email sent to military officials from Pakistan using the “Homeland Security Summit Middle East” conference as bait

- An email sent to Polish government employees [12] on August 11, 2014 had a MIME HTML (.MHT) file attachment named “MH17.doc,” which exploited CVE-2012-0158.



Exploit for CVE-2012-0158 disguised as a MIME HTML (.MHT) file

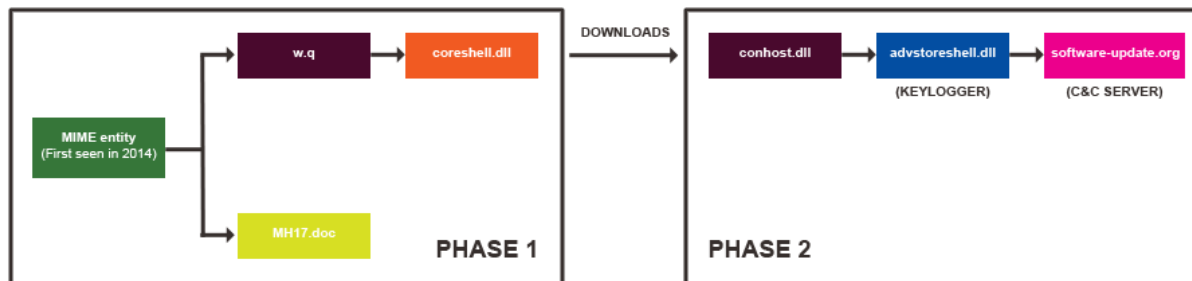
Attack Details

All of the observed Operation Pawn Storm attacks comprised several stages. Each attack had at least two phases:

- In phase 1, opening the email attachment displays a decoy document while the exploit runs in the background. The exploit drops a downloader component (.DLL file) named “netids.dll,” “netidt.dll,” or “coreshell.dll.”

- In phase 2, the downloader component communicates with a C&C server and downloads a dropper that ultimately installs a keylogger. After

capturing information from infected systems, the keylogger sends data back to the C&C server.



Phases 1 and 2 in an Operation Pawn Storm attack

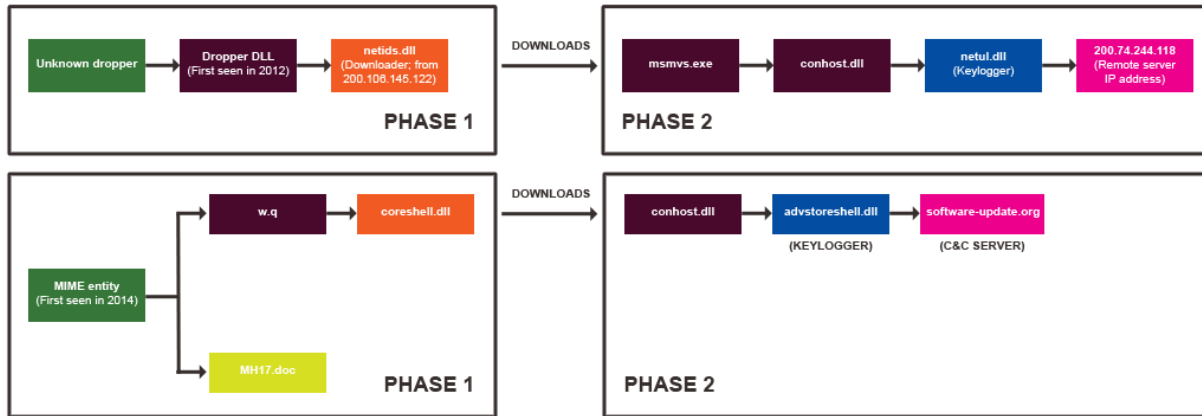
We only managed to collect latter-stage payloads for two out of the six aforementioned attacks. The C&C servers tied to the other four attacks refused to serve the rest of the files to complete the attack chains.

Multistage attacks are a double-edged sword. If one link in the attack chain, aside from the end node, is detected and removed in the initial infection stage, the entire attack fails. On the other hand, having several links in the attack chain makes detecting the final component more difficult. Tracing the previous and next links is also difficult when any of the components is inspected on its own outside the attack chain.

Although some of the C&C servers were still alive at the time of investigation, they did not respond to our infected systems. Repeated attempts to trick the C&C servers into serving the next files in the incomplete attack chains failed. The attacks they were tied to could be time sensitive and it is possible that they no longer hosted the files for succeeding stages.

Attack Evolution

Even though the filenames used for different components remained fairly consistent from 2010 to the present, earlier attacks were more elaborate and complex compared with those seen this year. The 2014 attacks we have seen were more streamlined.



Comparison of an Operation Pawn Storm attack in 2011 and another in 2014

Although variations in past and current attack chains exist, both are still being used by threat actors to date to ensure one

thing—detection evasion. The following table compares and contrasts the six Operation Pawn Storm attacks in greater detail.

Operation Pawn Storm Attack Comparison					
Case 1	Case 2	Case 3 [13]	Case 4	Case 5	Case 6
<p>Unknown exploit, possibly disguised as a .PDF, .DOC, or .RTF file, carries the top-level dropper (<i>dropper.exe</i>; SHA-1: <i>72cfd996957bde06a02b0adb2d66d8a9c25bf37</i>)</p>	<p>.RTF file exploits CVE-2010-3333 (SHA-1: <i>956d1a36055c903cb570890da69deabaacb5a18a</i>) and drops <i>saver.scr</i> (SHA-1: <i>e8b55d9aef124df4008b0d372bf2f2d3e5e5ae7</i>)</p>	<p>Unknown exploit carries a dropper (Dropper DLL; SHA-1: <i>9c622b39521183dd71ed2a174031ca159beb6479</i>)</p>	<p>Two .XLS files come with spear-phishing emails:</p> <ul style="list-style-type: none"> First file (<i>APEC Media list 2013 Part1.xls</i>; SHA-1: <i>a90921c182cb90807102ef402719ee8060910345</i>) exploits CVE-2012-0158 Second file (<i>APEC Media list 2013 Part2.xls</i>; SHA-1: <i>b3098f99db1f80e27aec0c9a5a625a edaab5899a</i>) is a decoy document 	<p>.RTF file (SHA-1: <i>78d28072fdabf0b5aac5e8f337dc768d07b63e1e</i>) exploits CVE-2012-0158 and drops <i>saver.scr</i> (SHA-1: <i>7FBB5A2E46FACD3EE0C945F324414210C2199FFB</i>) into <i><Local Settings>\Temp\</i></p>	<p>.MHT file drops:</p> <ul style="list-style-type: none"> <i>MH17.doc</i> (SHA-1: <i>DAE7FAA1725DB8192AD711D759B13F8195A18821</i>), a decoy document, into <i><Local Settings>\Temp\</i> <i>W.q</i> (SHA-1: <i>8DEF0A554F19134A5DB3D2AE949F9500CE3DD2CE</i>), a dropper, into <i><Local Settings>\Temp\</i>

Operation Pawn Storm Attack Comparison					
Case 1	Case 2	Case 3 [13]	Case 4	Case 5	Case 6
<p><i>Dropper.exe</i> drops:</p> <ul style="list-style-type: none"> Decoy file (<i>Letter to IAEA.pdf</i>; SHA-1: 6ad a11c71a5176a8 2a8898680ed1e aa4e79b9bc3) into <Local Settings>\Temp\ Downloader (<i>netids.dll</i>; SHA-1: c5ce5b7d10a ccb04a4e45c3a 4dcf10d16b192 e2f) into <Local Settings>\Application Data\ 	<p><i>Saver.scr</i> drops:</p> <ul style="list-style-type: none"> Decoy document (<i>Military Cooperation.doc</i>; SHA-1: 0E 12C8AB9B89B6 EB6BAF16C4B 3BBF9530067 963F) into <Local Settings>\Temp\ <i>Skype.exe</i> (SHA-1: 550AB D71650BAEA05 A0071C4E084A 803CB413C31), a SEDNIT variant, into <Local Settings>\Temp\ <i>Cryptmodule.exe</i> (SHA-1: 4B 8806FE8E0CB4 9E4AA5D8F877 66415A2DB1E9 A9) into <AppData>\Microsoft\Crypt\ 	<p>Dropper DLL drops <i>netids.dll</i> (SHA-1: dd 61530076152dae56 8b4834b1899212c9 6c1a02) into <Local Settings>\Application Data\</p>	<p><i>APEC Media list 2013 Part1.xls</i> drops <i>dw20.t</i> (SHA-1: ac6b 465a13370f87cf579 29b7cfd1e45c36945 85), a .DLL file</p>	<p><i>Saver.scr</i> drops:</p> <ul style="list-style-type: none"> <i>IDF_Spokesperson_Targeted_Attack_101012.doc</i> (SHA-1: F5 42C5F9259274 D94360013D14 FFBECC43AAE 552), a decoy document, into <Local Settings>\Temp\ <i>Install.exe</i> (SHA-1: BC58A 8550C53689C8 148B021C917F B4AECC62AC 1) into <Local Settings>\Temp\ 	<p><i>W.q</i> drops:</p> <ul style="list-style-type: none"> <i>Coreshell.dll</i> (SHA-1: A85513 97E1F1A2C014 8E6EADCB56F A35EE6009CA) into <Program Files>\Common Files\System\ <i>Tmp64.dat</i>, a copy of <i>coreshell.dll</i>, into <Program Files>\Common Files\System\

Operation Pawn Storm Attack Comparison					
Case 1	Case 2	Case 3 [13]	Case 4	Case 5	Case 6
<p><i>Netids.dll</i> communicates with a C&C server (200.106.145.122)</p>	<ul style="list-style-type: none"> • <i>Military Cooperation.doc</i> has been encoded using Cyrillic characters and opens in Word • <i>Skype.exe</i> drops: <ul style="list-style-type: none"> • Downloader (<i>netids.dll</i>; SHA-1: 6b875661a74c4673ae6ee89acc5cb6927ca5fd0d), a SEDNIT variant, into <Windows>\system32\ • Copy of <i>netids.dll</i> (<i>mcs.v.tmp</i>) into <Windows>\system32\ • <i>Cryptmodule.exe</i> drops <i>s.vbs</i> (actually a .PE and not a .VBS file) and communicates with a C&C server (<i>windows.kz</i>) 	<p><i>Netids.dll</i> downloads and saves <i>msmvs.exe</i> (SHA-1: 88f7e271e54c127912db4db49e37d93aea8a49c9) in <Local Settings>\Temp\</p>	<p><i>Dw20.t</i> drops <i>netids.dll</i> (SHA-1: 3814eec8c45fc4313a9c7f65ce882a7899cf0405)</p>	<p><i>Install.exe</i> drops <i>netids.dll</i> (SHA-1: 14BEEB0FC5C8C887D0435009730B6370BF94BC93) into <Windows>\system32\</p>	<p><i>Coreshell.dll</i> downloads <i>conhost.dll</i> (SHA-1: B49FAD3E5E6787E96373AC37ED58083F7572D72A), a dropper, from a C&C server</p>

Operation Pawn Storm Attack Comparison					
Case 1	Case 2	Case 3 [13]	Case 4	Case 5	Case 6
C&C server confirms receipt of communication from infected systems then stops further interactions	<ul style="list-style-type: none"> • <i>Netids.dll</i> communicates with a C&C server (70.85.221.20) • <i>S.vbs</i> (SHA-1: 0A3E6607D5E9C59C712106C355962B11DA2902FC) runs <code>CreateFile C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\update.exe</code> but does nothing else 	<i>Msmvs.exe</i> drops <i>conhost.dll</i> (SHA-1: 55318328511961EC339DFDDCA0443068DCCE9CD2) into <code><Local Settings>\Temp\</code>	<i>Netids.dll</i> communicates with a C&C server (70.85.221.10)	<i>Netids.dll</i> communicates with a C&C server (70.85.221.10)	<i>Conhost.dll</i> drops <i>advstoreshell.dll</i> (SHA-1: E338A57C35A4732BBB5F738E2387C1671A002BCB), a keylogger
		<i>Conhost.dll</i> drops <i>netui.dll</i> (SHA-1: 5A452E7248A8D3745EF53CF2B1F3D7D8479546B9), a keylogger, into <code><Windows>\system32\</code>			<i>Advstoreshell.dll</i> sends logs of stolen data to a C&C server (<i>software-update.org</i>)
		<i>Netui.dll</i> sends logs of stolen data to a C&C server (200.74.244.118)			

Next-Level Phishing Targets

The attackers used specially crafted emails to redirect targets to any of several phishing websites with domain names that were very similar to those of well-known conferences and media outfits. These websites did not host malicious content but visiting them did lead to the automatic execution of a nonmalicious JavaScript. Links to these fake websites were then embedded in spear-phishing emails and sent to selected targets.

Opening such an email and clicking the link in OWA redirected victims to legitimate websites. The JavaScript made it appear that the victims' OWA sessions ended while at the same time, tricked them into reentering their credentials. To do this, the attackers redirected victims to fake OWA log-in pages by setting their browsers' open windows property. The victims' credentials thus ended up in the attackers' hands.

Note that two special conditions need to be met for the attacks to succeed—victims should use OWA and click the embedded links via the web portal's preview pane. The attacks worked on any popular browser such as Firefox®, Safari®, Chrome™, and Internet Explorer®. No vulnerabilities need to be exploited for the JavaScript to work.

Because many companies allow employees to use webmail services to access their mailboxes while on business travel or at home, these attacks are likely to succeed. Once they do, attackers can gain access to compromised mailboxes that they can then use to gain a foothold in target networks.

Throughout the course of investigation, several targets have been identified, including:

- ACADEMI, formerly Blackwater (United States)
- Broadcasting companies in various

countries

- Military attachés from various countries
- Ministry of Defense (France)
- Ministry of Defense (Hungary)
- Multinational company based in Germany
- Organization for Security and Co-operation in Europe (OSCE) (Austria)
- Pakistani military officials
- Polish government employees
- SAIC (United States)
- U.S. Department of State
- Vatican Embassy (Iraq)

The following case studies reveal more in-depth details on four specific attacks.

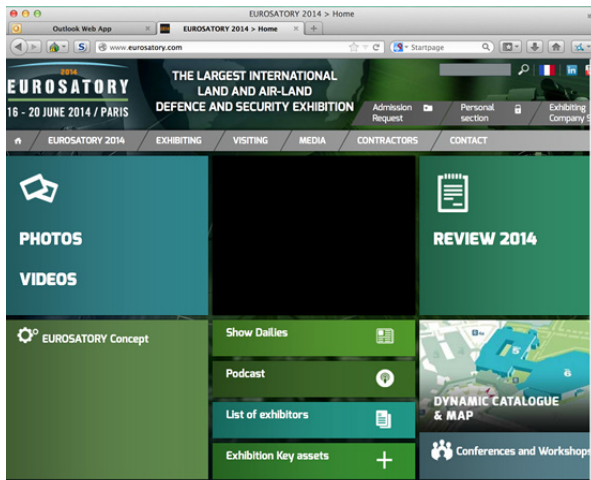
CASE 1: MINISTRY OF DEFENSE, HUNGARY

- **Malicious conference domain:** *eurosatory2014.com*
- **Real conference domain:** *eurosatory.com*
- **Phished OWA domain:** *mail.hm.gov.hu*
- **Real OWA domain:** *mail.hm.gov.hu*

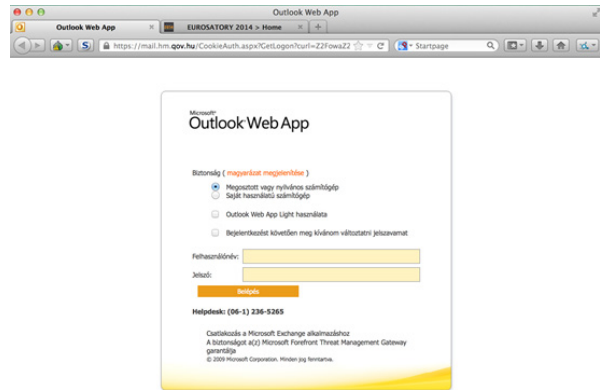
The attackers created a domain that was very similar to *eurosatory.com* [14], a website for an international land and air-land defense and security exhibition. They then sent emails with the link, *http://eurosatory2014.com*, to selected employees of the target defense ministry who might actually have been expecting to hear from the conference staff

members.

Clicking the link embedded in the email via the OWA preview pane opens the real conference website in a new tab. The victims' OWA session in the other tab, meanwhile, is redirected to a phished log-in page that makes it look like the session has ended.



Real “EUROSATORY 2014” conference website opens in a new tab after clicking the link in a spear-phishing email viewed in OWA



“Closed” OWA session page (fake) victims will see, forcing them to reenter their credentials

In reality, the victims’ OWA session did not end. The previously mentioned JavaScript just redirected them to a fake OWA log-in page that looks just like the Ministry of Defense in Hungary’s real one.

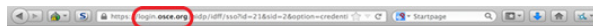
Apart from “EUROSATORY 2014,” other conferences were also used to target employees of the Ministry of Defense in Hungary as shown in the following table.

Similar Attacks Against the Ministry of Defense, Hungary		
Conference	Target Domain	Malicious Domain
“Africa Aerospace and Defence 2014”	<i>aadexpo.co.za</i>	<i>aadexpo2014.co.za</i>
“The 10th Special Operations Forces Exhibition & Conference”	<i>sofexjordan.com</i>	<i>sofexjordan2014.com</i>
“ITEC”	<i>itec.co.uk</i>	<i>itec2014.co.uk</i>

CASE 2: OSCE, AUSTRIA

- **Malicious news domain:** *vice-news.com*
- **Real news domain:** *news.vice.com*
- **Phished OWA domain:** *log-in-osce.org*
- **Real OWA domain:** *log-in.osce.org*

This attack targeted OSCE employees in Austria. Although the attackers used similar tactics, they did not spoof a conference website. They instead used a fake version of the news website, *news.vice.com*.



OSCE

Token Login

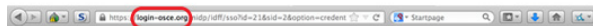
Username:

Token:

Log in

INFO: Token consists of your 4 digit PIN + PASSCODE

In case you are experiencing problems, please contact your Local ICT Support
Working hours: 9:00 - 17:00



OSCE

Login

Username:

Password:

Log in

AIS

In case you are experiencing problems please contact the ICT-Servicesdesk:
Working hours: 8:30 - 17:30 (Vienna Time)
Telephone: +43 1 51436 6500
ais

Comparison of the legitimate (top) and spoofed (bottom) OWA log-in pages of OSCE

Even though OSCE provides better security for webmail users compared with the other targets via one-time session token use during log-in, attackers can still steal highly sensitive data from victims by hijacking a single session.

CASE 3: SAIC, UNITED STATES

- **Malicious conference domain:** *natoexhibitionff14.com*

- **Real conference domain:** *natoexhibition.org*
- **Phished OWA domain:** *webmail-saic.com*
- **Real OWA domain:** *webmail.saic.com*

This attack targeting SAIC was very similar to the first case. The attackers spoofed the website of the “Future Forces 2014” conference to trick email recipients into handing over their webmail credentials.



Microsoft
Outlook Web App

Security ([show explanation](#))

This is a public or shared computer
 This is a private computer

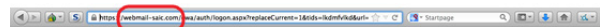
Use the light version of Outlook Web App

User name:

Password:

Log in

Connected to Microsoft Exchange
© 2010 Microsoft Corporation. All rights reserved.



Microsoft
Outlook Web App

Security ([show explanation](#))

This is a public or shared computer
 This is a private computer

Use the light version of Outlook Web App

User name:

Password:

Log in

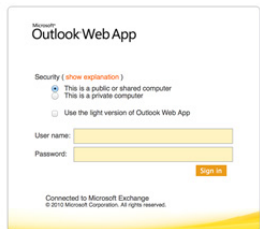
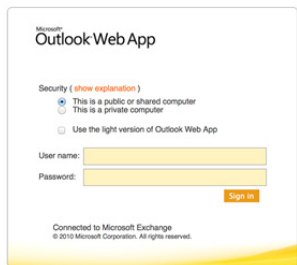
Connected to Microsoft Exchange
© 2010 Microsoft Corporation. All rights reserved.

Comparison of the legitimate (top) and spoofed (bottom) OWA log-in pages of SAIC

CASE 4: ACADEMI

- **Malicious news domain:** *tolonevvs.com*
- **Real news domain:** *tolonews.com*
- **Phished OWA domain:** *academl.com*
- **Real OWA domain:** *academi.com*

This attack targeted the employees of U.S. defense contractor, ACADEMI, using the same phishing tactics as in the second case.

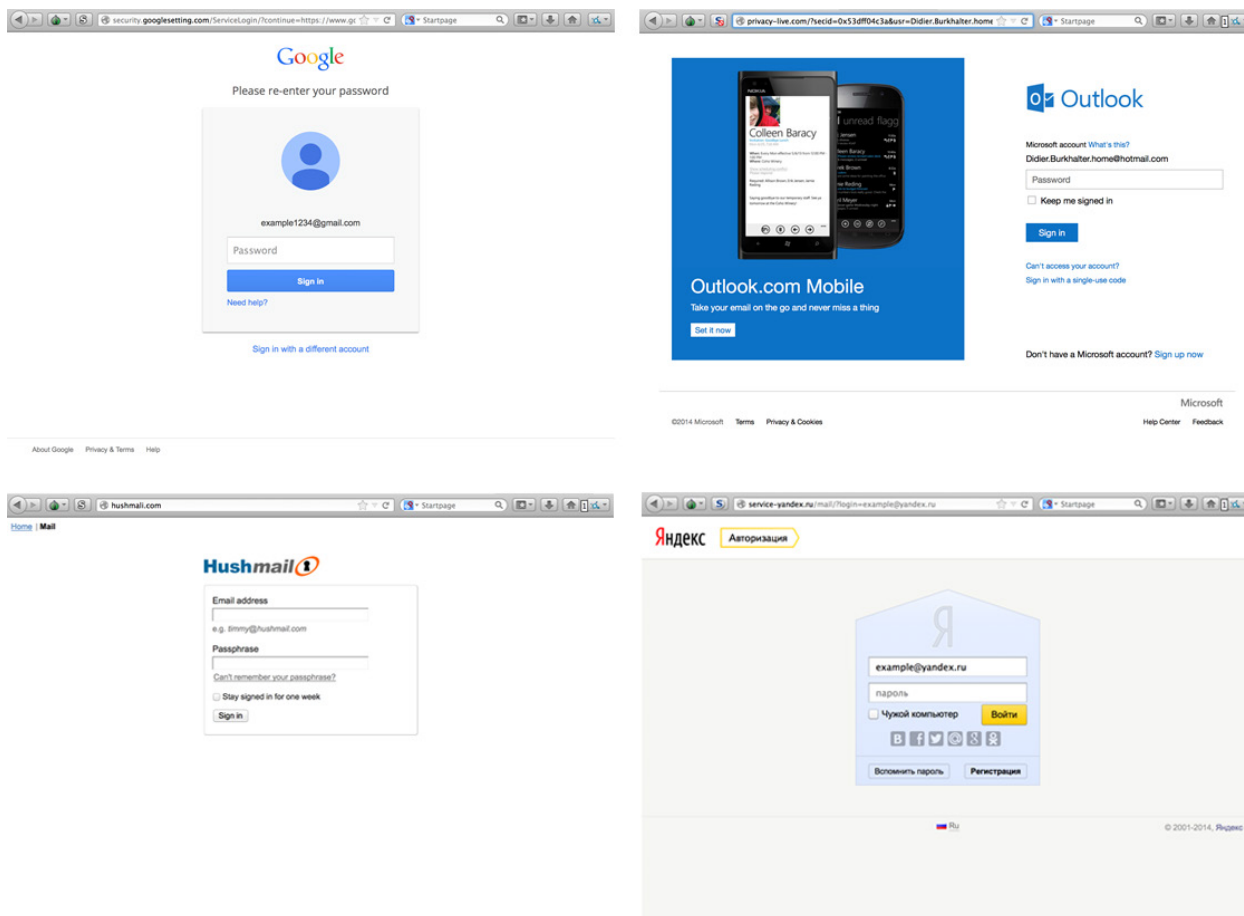


Comparison of the legitimate (top) and spoofed (bottom) OWA log-in pages of ACADEMI

Apart from the four specific cases presented above, evidence pointing to a fake OWA server for a multinational company based in Germany was also discovered. The threat actors registered a domain that looked very similar to the target's real domain and purchased a Secure Sockets Layer (SSL) certificate for the fake domain as part of preparations for a targeted attack. Trend Micro was able to warn the target early on, which helped thwart the threat.

Other Webmail Services

OWA users are not the only ones at risk though, as the threat actors behind Operation Pawn Storm also targeted users of free webmail services such as Gmail™, Live Mail, Yahoo!®, Hushmail, and Yandex.



Sample Gmail, Live Mail, Hushmail, and Yandex account phishing websites

We leaked specific credentials to the threat actors in a couple of cases to see if the fake webmail service log-in pages were indeed intended for attack use. Within minutes of leaking the test credentials, unauthorized log-ins were recorded. The first log-in was usually an automated log-in check from the same IP address as the phishing website's owner. The succeeding log-ins were made from the IP addresses,

46.166.162.90 (Latvia) and 192.154.110.244 (United States), via Internet Message Access Protocol (IMAP). No other forms of abuse such as sending spam via the compromised accounts were witnessed. This showed that the attackers were indeed trying to obtain sensitive data from their targets instead of using their accounts for fraud and other financially motivated scams.

CONCLUSION

Operation Pawn Storm used next-level spear-phishing tactics to obtain the email credentials of primarily military, embassy, and defense contractor personnel from the United States and its allies. The threat actors used a mix of spear-phishing emails and specially crafted webmail service phishing websites to gain access to victims' inboxes in hopes of getting better footholds inside target organizations. So as not to raise suspicion, the attackers used well-known events and conferences as social engineering bait. They have been quite persistent as well, as we have seen evidence that attacks have been going on since 2007.

Apart from effective phishing tactics, the threat actors used a combination of proven targeted attack staples to compromise systems and get in to target networks—exploits and data-stealing malware. SEDNIT variants particularly proved useful, as these allowed the threat actors to steal all manners of sensitive information from the victims' computers while effectively evading detection.

Trend Micro has notified the targets that have been identified in this paper. Individuals and their respective organizations, meanwhile, should use solutions that can help protect against the various attack vectors that the threat actors behind Operation Pawn Storm used.

Messaging security solutions such as Trend Micro™ InterScan™ Messaging Security [15] and the ScanMail™ Suite for Microsoft Exchange [16] can send suspicious email attachments to a sandbox for analysis, thus protecting recipients from threats. Other products such as OfficeScan™ [17] for endpoints and InterScan Web Security Virtual Appliance [18] for gateways can also block user access to known phishing sites.

For overall protection against targeted attacks, Trend Micro™ Deep Discovery [19] can help protect potential targets by sandboxing and analyzing suspicious attachments to identify phishing emails via Email Inspector. Via 360-degree monitoring of network traffic to get networkwide visibility and intelligence, Deep Discovery allows users to detect and respond to targeted attacks and advanced threats. It also monitors all ports and more than 80 protocols, giving users the broadest protection available. Even more, specialized detection engines and custom sandboxing help identify and analyze malware, C&C communications, and evasive attacker activities that are invisible to standard security solutions. Along with in-depth threat intelligence, it allows for rapid response and automatic sharing with other security products to create real-time custom defense against attacks.

REFERENCES

- [1] Trend Micro Incorporated. (2014). *Threat Encyclopedia*. “SEDNIT.” Last accessed October 13, 2014, <http://about-threats.trendmicro.com/us/search.aspx?p=SEDNIT>.
- [2] Symantec Corporation. (1995–2014). *Symantec*. “Infostealer.Sofacy.” Last accessed October 17, 2014, http://www.symantec.com/security_response/writeup.jsp?docid=2011-090714-2907-99&tabid=2.
- [3] Trend Micro Incorporated. (2014). *Threat Encyclopedia*. “BKDR_SEDNIT.AE.” Last accessed October 13, 2014, http://about-threats.trendmicro.com/us/malware/BKDR_SEDNIT.AE.
- [4] Trend Micro Incorporated. (2014). *Threat Encyclopedia*. “BKDR_SEDNIT.SM.” Last accessed October 13, 2014, http://about-threats.trendmicro.com/us/malware/BKDR_SEDNIT.SM.
- [5] Trend Micro Incorporated. (2014). *Threat Encyclopedia*. “TROJ_SEDNIT.TOK.” Last accessed October 13, 2014, http://about-threats.trendmicro.com/us/malware/TROJ_SEDNIT.TOK.
- [6] Wikimedia Foundation Inc. (March 16, 2014). *Wikipedia*. “Pawn Storm.” Last accessed October 21, 2014, http://en.wikipedia.org/wiki/Pawn_storm.
- [7] The MITRE Corporation. (1999–2014). *CVE*. “CVE-2010-3333.” Last accessed October 16, 2014, <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3333>.
- [8] Trend Micro Incorporated. (2014). *Threat Encyclopedia*. “TROJ_ARTIEF.” Last accessed October 21, 2014, http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/TROJ_ARTIEF.
- [9] Post Staff. (January 9, 2012). *New York Post*. “Three Car Bombs Explode in Iraq, Killing 17.” Last accessed October 16, 2014, <http://nypost.com/2012/01/09/three-car-bombs-explode-in-iraq-killing-17/>.
- [10] The MITRE Corporation. (1999–2014). *CVE*. “CVE-2012-0158.” Last accessed October 16, 2014, <http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0158>.
- [11] IQPC. (2014). *Homeland Security Summit Middle East*. “Towards Total Preparedness: Advancing Command and Control and Communication for Increased Identification, Access, Surveillance, Cyber Protection Capabilities.” Last accessed October 16, 2014, <http://www.homelandsecurityme.com/>.
- [12] *Malware@prevenity*. (September 11, 2014). “mht, MS12-27 oraz *malware*.info.” Last accessed October 16, 2014, <http://malware.prevenity.com/2014/08/malware-info.html>.
- [13] R136a1. (December 27, 2012). *Analyzing Unknown Malware*. “#3 Disclosure of Another 0-Day Malware—Update and Additional Information.” Last accessed October 17, 2014, http://thegoldenmessenger.blogspot.ro/2012/12/3-disclosure-of-another-0day-malware_27.html.
- [14] COGES. (2013). *EUROSATORY 2014*. “The Largest International Land and Air-Land Defence and Security Exhibition.” Last accessed October 17, 2014, <http://www.eurosatory.com/>.
- [15] Trend Micro Incorporated. (2014). *Trend Micro*. “InterScan Messaging Security.” Last accessed October 21, 2014, <http://www.trendmicro.com/us/enterprise/network-security/inter-scan-message->

security/.

- [16] Trend Micro Incorporated. (2014). *Trend Micro*. "ScanMail Suite for Microsoft Exchange." Last accessed October 21, 2014, <http://www.trendmicro.com/us/enterprise/network-web-messaging-security/scanmail-microsoft-exchange/>.
- [17] Trend Micro Incorporated. (2014). *Trend Micro*. "OfficeScan—Endpoint Protection." Last accessed October 22, 2014, <http://www.trendmicro.com/us/enterprise/product-security/officescan/>.
- [18] Trend Micro Incorporated. (2014). *Trend Micro*. "InterScan Web Security Virtual Appliance." Last accessed October 22, 2014, <http://www.trendmicro.com/us/enterprise/network-security/interscan-web-security/virtual-appliance/>.
- [19] Trend Micro Incorporated. (2014). *Trend Micro*. "Deep Discovery Advanced Network Security." Last accessed October 21, 2014, <http://www.trendmicro.com/us/enterprise/security-risk-management/deep-discovery/>.

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

©2014 by Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.



Securing Your Journey
to the Cloud

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.

Phone: +1.817.569,8900