proofpoint™

Proofpoint Threat Report

July - September 2015

The Proofpoint Threat Report explores threats, trends, and transformations that we see within our customer base and in the wider security marketplace.

Executive Summary

The Proofpoint Threat Report examines threats, trends, and transformations that Proofpoint researchers observe in the threat landscape. The Threat Report for the quarter covering the July-September 2015 timeframe shows that cybercriminals did not take the summer off. The top findings of Proofpoint research for the quarter include:

- Campaigns distributing the Dridex banking Trojan dwarfed other malware payloads in volume, and continued to innovate with adaptations in attachment formats, document templates, obfuscation, and other infection techniques.
- The September pause in Dridex activity demonstrated the speed with which threat actors can adapt and change payloads, and delivery methods.
- Threat actors behind targeted attacks continue to leverage email as the preferred vector for gaining a foothold in their targeted organizations. In particular, the continued increase in phishing activity known as “Business Email Compromise” (BEC), also referred to as “wire transfer fraud,” reached a level sufficient to provoke a warning from the FBI about this threat.
- Angler dominates the exploit kit landscape, with only four others (Neutrino, Nuclear, Magnitude, and RIG) accounting for most of the rest of the EK activity. However, new exploit kits continue to enter the space and integrate the most recent exploits, creating more options for threat actors and a wider variety of threats confronting organizations.
- Fraudulent social media account activity has become a major risk for organizations and individuals, as attackers aggressively embrace techniques for hijacking customer support conversations to steal personal and financial information.
- Data breaches dominated the headlines in the information security world in Q3, with multiple high-profile breaches exposing not only highly sensitive personal information for up to 35 million individuals, but also details of several previously undisclosed zero-day exploits that quickly made their way into exploit kits and other threat actor tools.

Organizations need to take action to defend themselves against this wide range of threats; immediate actions include:

- Adopt advanced threat solutions to identify and block targeted attacks that travel over email, the #1 threat vector.
- Deploy automated incident response capabilities to rapidly identify and mitigate infections, including detecting and blocking command and control (C2) communication of infected systems.
- Patch client systems for all known operating system and application vulnerabilities to protect against aggressive exploit kits that reach clients via email, malvertising, and drive-by downloads.
- Update both email gateway rules and internal financial controls in order to improve resistance against wire transfer fraud scams.
- Police social media activity for potentially fraudulent accounts that can hijack conversations with customers and steal personal and financial information.

Threats

Proofpoint threat data for Q3 2015 captured key developments in areas from advanced threats and exploit kits to social media.

Advanced Threats

Proofpoint's insight into advanced threat data on malware and campaigns in July-September demonstrate several clear trends over the quarter. The top takeaways from Proofpoint research were:

- Dridex campaigns continued in full swing through the summer
- Dridex arrests disrupt campaigns, prompt change in payloads
- APT actors leverage phishing to infect targets
- High volume of "Business Email Compromise" (BEC) messages

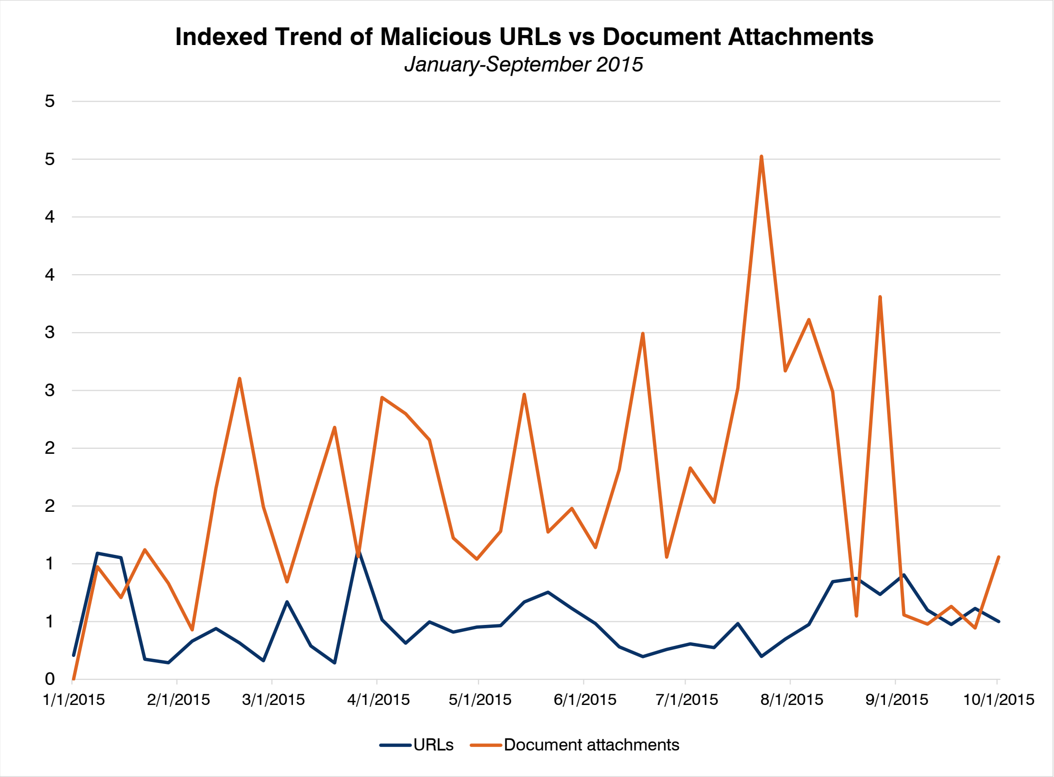
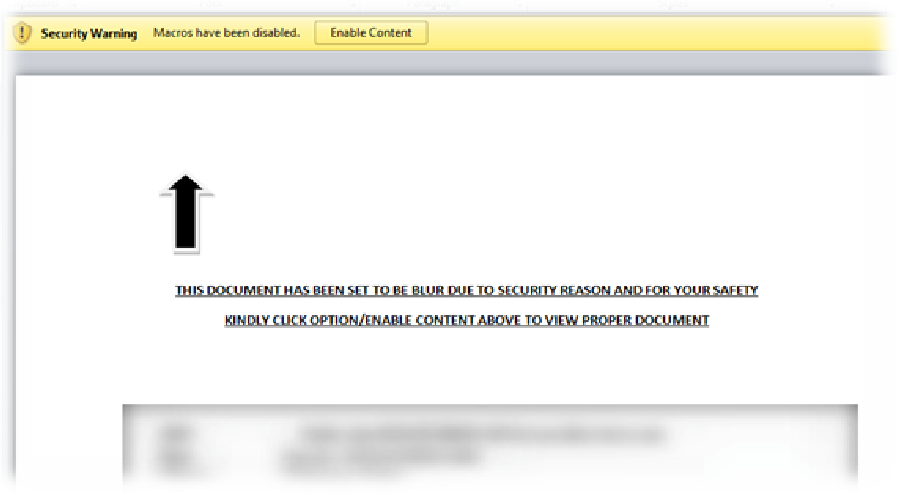


Figure 1: Indexed trend of malicious URLs vs document attachments, January-September 2015

Dridex campaigns continued in full swing through the summer

Proofpoint data show that after switching in late 2014 from primarily URL-driven campaigns to the use of document attachments to deliver payloads, threat actors continued to heavily favor these attachment-based campaigns. (Fig. 1)

For the better part of the summer, the volume of document attachments far outweighed that of malicious URLs in unsolicited email campaigns. As summarized in our [mid-year Threat Report](), these campaigns employed malicious macros of increasing sophistication embedded in a [variety of document formats](). The documents themselves leveraged social engineering techniques in order to entice the recipient to click the "Enable Content" button that would allow the malicious macro to run and install the malware payload(s). (Fig. 2)



Security Warning Macros have been disabled.

THIS DOCUMENT HAS BEEN SET TO BE BLUR DUE TO SECURITY REASON AND FOR YOUR SAFETY

KINDLY CLICK OPTION/ENABLE CONTENT ABOVE TO VIEW PROPER DOCUMENT

Figure 2: Example of attached document with malicious macro. User is instructed to click "Enable Macros" to reveal the (fake) blurred content

By July, the relatively rudimentary document templates detected in the early months of these campaigns had been succeeded by professional-looking documents that used a pretense of ”security features” (such as blurring or encoding) to trick the end-user into running the embedded code and enabling the infection of their system.

Spreading primarily Dridex, the massive volume of these document attachment campaigns dwarfed other malware campaigns. (Fig. 3)

While the Dridex campaigns mostly targeted organizations in the US and UK during the first half of 2015, by mid-year they started to target other countries in the EU. For the entire month of July, France in particular was targeted by Dridex campaigns, as noted by Proofpoint researchers:

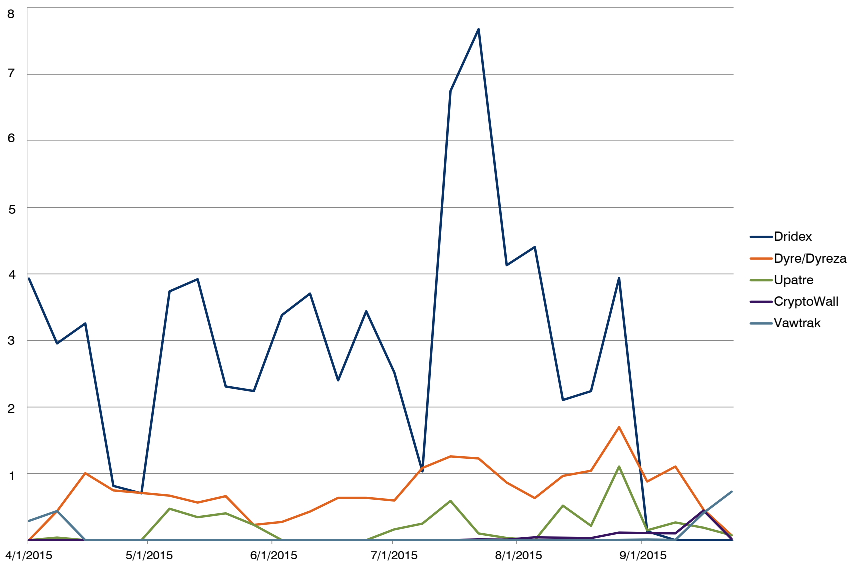


Figure 3: Indexed weekly phishing document attachment malware volume, by payload, April-September 2015

- Dridex actor shifts focus to Europe, including first wave of French campaigns: http://www.proofpoint.com/us/threat-insight/post/not-so-innocents-abroad-dridex-actor-shifts-focus-to-europe
- Analysis of sustained Dridex campaigns targeting France: http://www.proofpoint.com/us/threat-insight/post/Fleurs-du-malware

As the data show, in August the volume of Dridex messages continued and actually increased, but attackers again distributed their focus more broadly.

Dridex arrests disrupt campaigns, prompt change in payloads

August was followed by another noteworthy event of the third quarter: the reported arrests of several individuals in the Dridex malware group around September 1. There was speculation at the time regarding the impact this would have on Dridex campaign activity, and as Proofpoint data for the quarter show, the impact was pronounced and almost immediate.

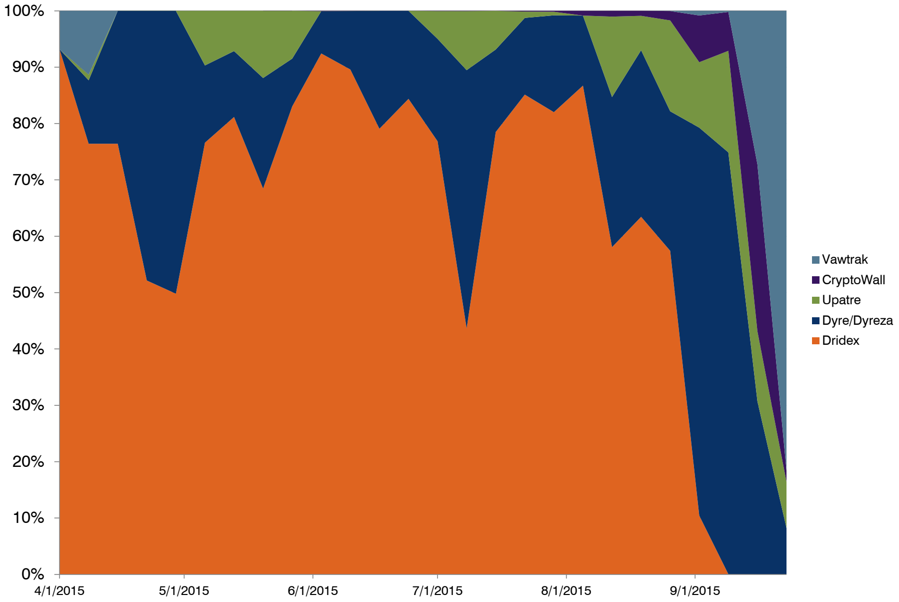


Figure 4: Weekly phishing document attachment malware payload as a percentage of total malware, April-September 2015

But what happened to malware payloads during the Dridex hiatus? Did they remain the same, or did the absence of Dridex create an opportunity for other malware authors, a vacant niche in the malware ecosystem, so to speak? Looking at the chart in Figure 3 above, it appears that the volumes of other payloads remained unaffected by the Dridex hiatus, but the relative volume of Dridex obscures variations in other payloads. Charting the most common malware payloads as a percentage of total activity gives a better view. (Fig. 4)

Viewed from this angle, it becomes evident that the main beneficiaries of the Dridex hiatus were initially Dyre (aka Dyreza, often seen with Upatre) and CryptoWall 3.0, which then ceded to a resurgent Vawtrak. Moreover, Dyre has been steadily present and exhibited brief surges over the past ten months, but CryptoWall and Vawtrak had both been largely absent from malicious document attachment phishing payloads in significant numbers for at least six months, so in raw terms these two were the most direct beneficiaries of the Dridex hiatus. Even if their overall volume did not approach that of the Dridex campaigns, the sudden change in payload can represent a significant challenge for defenses that have adapted to months of Dridex payloads.

(Proofpoint and others noted that the Dridex campaigns resumed on October 1. We will look more closely at this renewed activity in the Threat Report for October-December.)

Analysis of phishing malware payloads during the Dridex hiatus thus highlights several key traits:

- Threat actors are adept at substituting one ecosystem component for another, and there are many options available to them at any given time.
- “Old” threats are never far away: just because a particular malware payload has not been detected in months does not mean that it is no longer a threat.
- Malware is flexible: payloads that normally spread via one vector – such as CryptoWall via malvertising – can quickly ‘jump’ to other distribution vectors when the need and opportunity arise.

APT actors leverage phishing to infect targets

In addition to detecting and analyzing numerous broad-based campaigns this quarter, Proofpoint researchers carried out original analyses of highly targeted attacks.

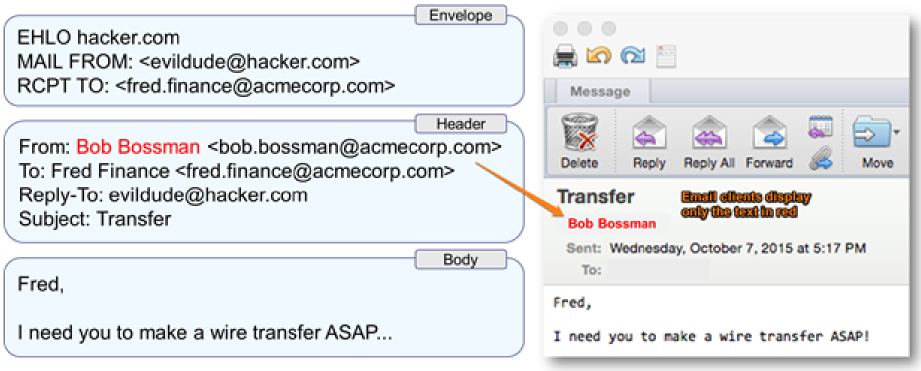
- In “In Pursuit of Optical Fibers and Troop Intel: Targeted Attack Distributes PlugX in Russia,” researchers examine a highly targeted campaign that uses specially crafted URLs and social engineering to spread the PlugX Trojan to targets in the Russian military and telecommunications sectors. Read more: http://www.proofpoint.com/us/threat-insight/post/PlugX-in-Russia
- In “Operation Arid Viper Slithers Back into View,” Proofpoint researchers detect and analyze an update to the Operation Arid Viper malware campaign. Read more: https://www.proofpoint.com/us/threat-insight/post/Operation-Arid-Viper-Slithers-Back-Into-View

Both attacks bear the characteristics of sophisticated state-sponsored actors and target individuals and organizations in narrowly-defined regions and verticals; both also demonstrate that email remains the “go-to” vector for these attacks.

As these threats show, attackers continue to employ increasingly sophisticated techniques against new targets in order to find and steal sensitive information. Organizations need to recognize that they cannot rely on traditional antivirus and anti-spam solutions to detect and stop these advanced threats. In order to combat targeted attacks, organizations should adopt next-generation solutions that make it possible to identify and respond to sophisticated targeted attacks by correlating advanced detection with threat intelligence about actor TTPs and global views of threat traffic, including IOCs that enable response teams to quickly detect and mitigate compromises. Moreover, a multi-layer approach is essential, with email security representing the logical starting point for an advanced threat defense: like this targeted attack, email remains the vector-of-choice for penetrating target organizations and delivering these sophisticated payloads.

High volume of “Business Email Compromise” (BEC) messages

The period of July-September also witnessed the continued increase in phishing activity known as “Business Email Compromise” (BEC), also referred to as “wire transfer fraud,” which reached a level sufficient to provoke a warning from the FBI about this threat. While some BEC phishing messages include a malicious URL or attachment, many feature simple text emails to an individual with purchasing authority, often at the executive level, and sometimes a spoofed sender address. (Fig. 5)



EHLO hacker.com
MAIL FROM: <evildude@hacker.com>
RCPT TO: <fred.finance@acmecorp.com>

From: Bob Bossman <bob.bossman@acmecorp.com>
To: Fred Finance <fred.finance@acmecorp.com>
Reply-To: evildude@hacker.com
Subject: Transfer

Fred,

I need you to make a wire transfer ASAP...

Transfer
Bob Bossman
Sent: Wednesday, October 7, 2015 at 5:17 PM
To:

Fred,

I need you to make a wire transfer ASAP!

Figure 5: Visible and hidden message data in a BEC phishing email

This is a low-volume social engineering attack in which the simplicity and apparent legitimacy of the BEC phishing message are important factors. The visible “From” line of the message often bears the name of the CEO or other high-ranking executive in the targeted organization. The message typically requests that the recipient immediately make a wire transfer to a third party, often with instructions to keep the request and transfer confidential. If multiple messages are used, the first will be brief and have few details; subsequent messages will include instructions for bank routing and other details. The header, envelope sender, and “From” display name may be spoofed, while the “Reply to” address will be that of the attacker. These emails frequently also leverage fraudulent domain names that closely mimic that of the targeted organization.

These attacks embrace a “blockbuster” approach on the part of the attackers, in that while many of these messages will be quickly recognized by recipients as phishing, the small fraction that succeed can yield millions of dollars in fraudulent transfers.

Defending against this threat requires that organizations employ a combination of technology solutions and procedural controls.

- Configure email gateway rules to flag inbound messages that spoof the organization’s domain, use Subject tagging for commonly used keywords such as “transfer”, and Display Name matching for commonly targeted recipients.
- Leverage email authentication techniques such as SPF, DKIM, and DMARC to flag BEC messages when they fail authentication.
- Tag the Subject line of all inbound email from the Internet with “EXTERNAL”, and reject all mail coming from an unresolvable domain in the envelope Sender field.
- Ensure that internal Finance and Purchasing controls are in place to authenticate legitimate requests, including addition of a secondary approval by another individual in the organization. Moreover, these controls should be out-of-band, requiring an in-person or telephone confirmation, rather than via email.
- Conduct culture training to all employees emphasizing that money transfers should never be carried out based solely on an email request.

As organizations learn to recognize and block – through a combination of technical and procedural means – BEC phishing messages, their impact will decrease. However, as Proofpoint research has shown, cybercriminals are capable of rapidly adapting to improved defenses and deploying new techniques and malware.

Exploit Kits

Exploit kit (EK) activity tracked by Proofpoint researchers in Q3 showed that Angler accounted for the majority of EK traffic over the quarter. (Fig. 6)

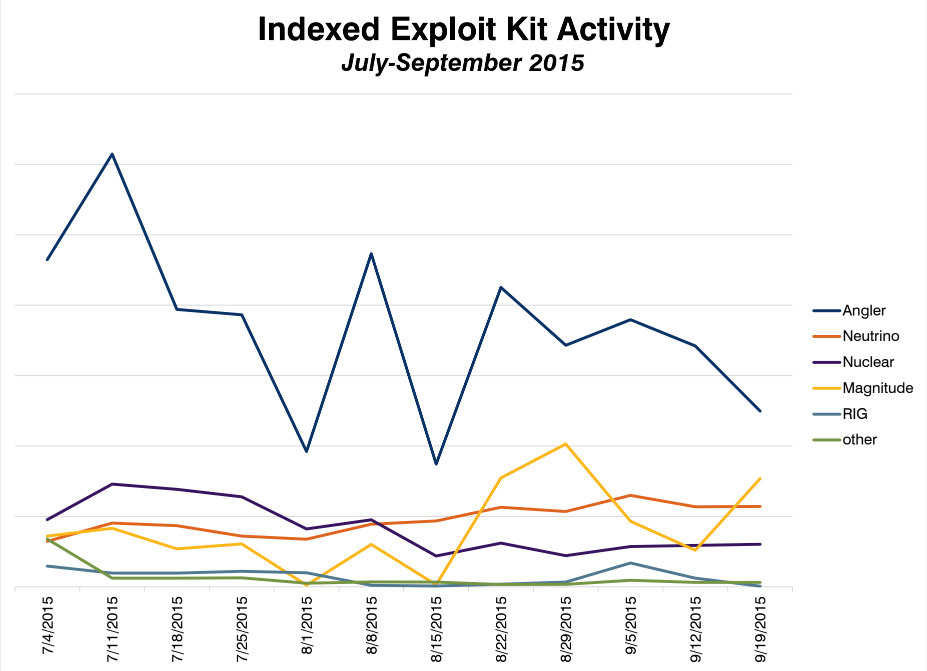


Figure 6: Top exploit kits by traffic, July-Sept 2015

Viewed as a percentage of total exploit kit traffic, Angler was even more prominent in the most recent quarter. The majority of the remaining traffic was divided between the Neutrino, Nuclear, and Magnitude exploit kits, with a number of smaller EKs contributing to the last 2-3% of EK traffic. (Fig. 7)

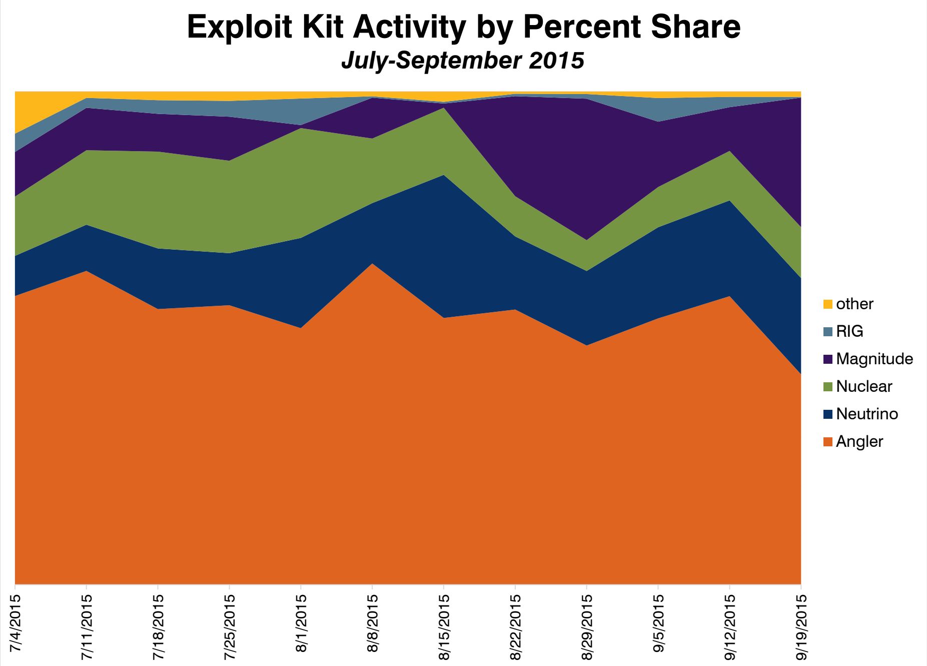


Figure 7: Exploit kit activity by percent share, July-September 2015

Exploit kits continued to update by integrating exploits targeting recently announced vulnerabilities, with the majority of exploits targeting Microsoft® platforms. (Table 1)

CVE	Targeted Platform	Integrated to EK
CVE-2015-1671	Microsoft Silverlight (MS15-044)	Angler, Magnitude
CVE-2015-5560	Adobe Flash integer overflow, impacts Microsoft Windows and Apple Mac OS X	Angler, Nuclear Pack
CVE-2015-2419	Microsoft Internet Explorer (MS15-065)	Angler, Magnitude, Neutrino, Hunter EK, RIG, Nuclear Pack
CVE-2015-2426	Adobe Type Manager library for Microsoft Windows (MS-15-078); enables local privilege escalation	Magnitude
CVE-2015-2444	Microsoft Internet Explorer (MS15-079)	Xer (aka Sundown)

Table 1: Exploit kit exploit integration, July-September 2015

During this period, significant EK developments noted by Proofpoint and other researchers included:

- Nuclear Pack and Angler added the Diffie-Hellman key exchange to prevent the replay of exploits by researchers. Read more: https://securelist.com/blog/research/72097/attacking-diffie-hellman-protocol-implementation-in-the-angler-exploit-kit/.
- Exploit kits filtered client traffic with expanded techniques for detecting antivirus and researcher tools such as local proxies.
- Geo-targeted malvertising shifted to high-profile sites, where previously the majority of this behavior was through pornographic websites.
- New “exploit kit” dubbed Spartan by Dell SecureWorks, which resembles a Nuclear Pack “detachable” flash.
- Attackers leveraged the Adobe® Type Manager® exploit (CVE-2015-2426) inside exploit kits to allow privilege escalation.

Relatively new exploit kits continued to enter the fray in Q3, with Hunter EK emerging and Sundown (analyzed by Proofpoint in June, Fig. 8) adding features and exploits before other exploit kits.

Related reading:

http://www.symantec.com/connect/blogs/sundown-exploit-kit-adds-internet-explorer-exploit-any-other-kit

http://www.proofpoint.com/us/threat-insight/post/Light-After-Dark

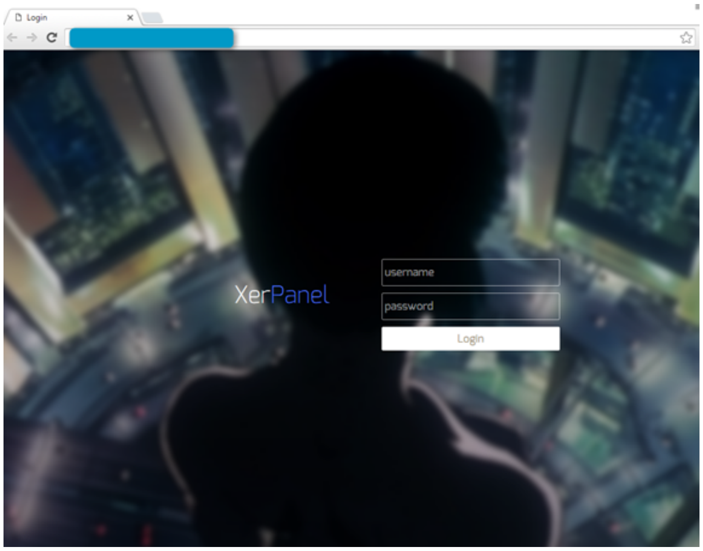


Figure 8: Xer (aka Sundown) exploit kit cpanel login page

http://www.proofpoint.com/us/threat-insight/post/Hunter-Exploit-Kit-Targets-Brazilian-Banking-Customers

Social Media

One of the more alarming social media security trends that Proofpoint Nexgate researchers observed in Q3 was the use of fraudulent social media accounts of major brands to phish customer account credentials. Specifically, fake customer care accounts redirected Customer Support inquiries from major retail banks to bogus web sites designed to harvest account credentials. Here's a quick sketch of the scheme:

1. A customer tweets a question to a bank's Twitter customer care account. For example, a customer tweets: "@MajorBankHelp – My phone's banking app stopped working"

2. An attacker monitoring @MajorBankHelp sees the question and tweets a "response" directly to the customer from a fake twitter account with a slightly different name. For example, the fake name might be @MajorBank_Help. The account is otherwise identical (same logo, images, text etc.) and is virtually indistinguishable from the real account.

3. The attacker's tweet includes a link to a bogus website, which also mimic's MajorBank's legitimate site, asking the customer to login to resolve their issue (e.g. download a fix). When the customer logs in to the bogus site, the attacker captures credentials to the customer's actual bank account.

We have seen this tactic applied not only to banks, but to retail, technology, and entertainment brands as well. It's an example of how the detailed context provided by social media enables bad actors to craft highly effective attacks. Not only does the phishing lure described above appear completely legitimate, but it's a message that the victim is actually expecting and incented to act upon (they want their problem solved)! It's a far cry from a random email lure from out of nowhere. Additional details about fraudulent social media account phishing and other social media are available on Proofpoint's Threat Insight blog.

Spam Statistics

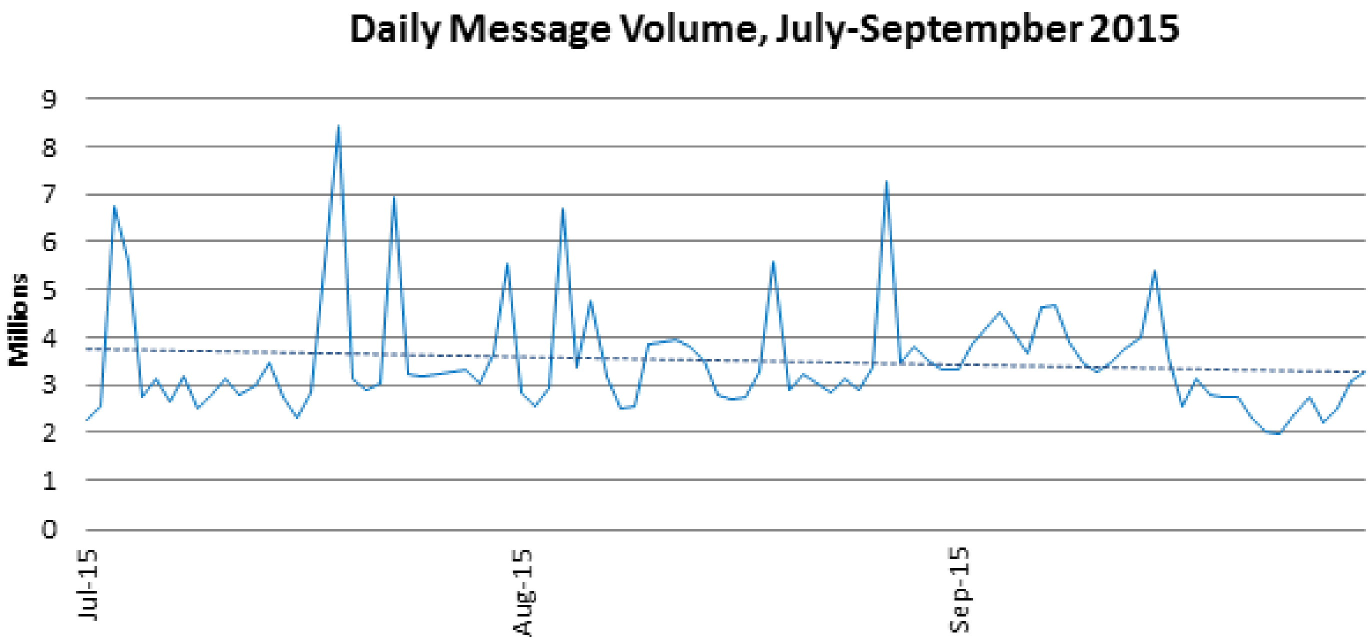


Figure 9: Daily spam message volume, July-September 2015

Proofpoint tracks spam volumes via a system of honeypots. The volumes historically align with that seen in our customer base. The daily message volume for the third quarter of 2015 follows.

Spam Sources by Region and Country

The table below details the percentage of total spam volume for the third quarter of 2015. The calculation for the EU is based on the inclusion of all member states, thereby producing a better representation of its volume. At 25.75%, the EU generated the majority of the world's spam. The remaining four countries in the top five slots were collectively responsible for 24.32%—insignificantly below the output of the EU.

Q3 2015		
1	EU	25.75%
2	U.S.	11.46%
3	China	6.41%
4	Russia	3.61%
5	Vietnam	2.84%

The following table displays the top five spam-sending member states of the European Union (EU) for the third quarter (2015), in addition to the percentage of total spam volume for each country.

Q3 2015		
1	Germany	3.20%
2	Spain	2.34%
3	Romania	2.20%
4	Italy	1.94%
5	Bulgaria	1.34%

News and Trends

Data breaches dominated the headlines in the information security world in Q3, with multiple high-profile breaches exposing not only highly sensitive personal information for up to 35 million individuals, but also details of several previously undisclosed zero-day exploits that quickly made their way into exploit kits and other threat actor tools.

Over 20 million records exposed in Office of Personnel Management (OPM) data breach

Millions of Social Security numbers were stolen from the databases of the Office of Personnel Management (OPM), an independent agency of the United States government. To make matters worse, in the midst of the PII breach, the OPM disclosed that the biometric data, including fingerprint records, of millions were stolen. This is especially disconcerting because biometric data cannot be changed, which means that once compromised, the disclosure cannot be remediated.

Read more: https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/

AshleyMadison data breach discloses millions of user records

The privacy of members of online dating service Ashley Madison was breached as hackers infiltrated ashleymadison.com and stole private information. Lawsuits involving hundreds of millions of dollars were filed in the wake of users' private information having been publicly disclosed.

Read more: http://www.theguardian.com/technology/2015/aug/22/adultery-website-ashley-madison-faces-578m-class-action-over-data-breach

Hacking Team data breach discloses zero-day exploits

The tables turned for notorious Italian cybersecurity firm Hacking Team, who were victimized by a hack. Hacking Team sells intrusion and surveillance technology to national governments and law enforcement agencies, which then allows them to access the computers of persons of interest. At least three zero-day exploits have been uncovered among the trove of data leaked by the perpetrator who breached Hacking Team.

http://www.csoonline.com/article/2943968/data-breach/hacking-team-hacked-attackers-claim-400gb-in-dumped-data.html

http://www.wired.com/2015/07/hacking-team-leak-shows-secretive-zero-day-exploit-sales-work/

IRS data breach exposes taxpayer returns

The IRS was breached and the number of potential victims stands at more than 334,000. Criminals used data stolen from other sources to gain access to taxpayers' past returns through the IRS "Get Transcript" application. This data will likely enable the continued growth of fraudulent tax returns next year.

Read more: http://www.cnbc.com/2015/08/17/irs-breach-affected-2x-as-many-taxpayers-as-expected.html

US Federal cybersecurity legislation advances

Backers of a bill called the Cybersecurity Information Sharing Act (CISA) will attempt to pass the bill to initiate the sharing of cyberthreat communication. CISA would protect businesses that share this information with each other, and with government agencies.

Read more: http://www.cio.com/article/2980699/cisa-likely-coming-back-to-senate-amid-doubts-about-effectiveness.html

Appendix: Proofpoint Threat Insight research published in Q3

"The Human Factor 2015 Close-up: What are users clicking on?" (July 1, 2015)

Threat Insight takes a closer look at the changes in phishing lures and templates that are targeting corporate users.
Threats analyzed: Phishing
http://www.proofpoint.com/us/threat-insight/post/What-Are-Users-Clicking-On

"Fleurs du malware": Phishing campaigners fill their nets in France (July 13, 2015)

Malicious macro phishing campaigns aggressively targeted France for the entire month of July, and this analysis looks at the techniques they used to spread Dridex and other banking Trojans.
Threats analyzed: Dridex, phishing, malicious macros
http://www.proofpoint.com/us/threat-insight/post/Fleurs-du-malware

"The Missing .LNK: Dridex Actor Tries New File Format" (July 29, 2015)

Dridex campaigners continue to experiment with file formats and other techniques to evade detection, in this case resurrecting link (LNK) files.
Threats analyzed: Dridex Banking Trojan, Phishing, Attachments
https://www.proofpoint.com/us/threat-insight/post/The-Missing-LNK

"Dead phish bounce: Alerting to brand risk with email backscatter" (August 6, 2015)

A quick look at how organizations can use email "bounce" messages to become aware of phishing campaigns that leverage their domains and brands.
Threats analyzed: Phishing, malvertising
http://www.proofpoint.com/us/threat-insight/post/Dead-Phish-Bounce

"Proofpoint Threat Report: Top trends of 2015 so far" (August 13, 2015)

Proofpoint threat researchers examine the threat landscape and highlight the top developments in the first half of 2015.
Threats analyzed: Dridex, phishing, malicious macros, social media phishing
http://www.proofpoint.com/us/threat-insight/post/Top-Trends-of-2015

"You Dirty RAT: Analyzing an AlienSpy payload" (August 14, 2015)

Proofpoint researchers reveal and analyze the obfuscation techniques and features of the AlienSpy RAT associated with a political scandal in Argentina.
Threats analyzed: AlienSpy, Remote access Trojans, Obfuscation
http://www.proofpoint.com/us/threat-insight/post/You-Dirty-RAT

"Hunter Exploit Kit Targets Brazilian Banking Customers" (August 27, 2015)

The Hunter exploit kit (EK) is detected and analyzed via its initial target of Brazilian banking customers.
Threats analyzed: Hunter EK, Phishing, Banking Trojans
https://www.proofpoint.com/us/threat-insight/post/Hunter-Exploit-Kit-Targets-Brazilian-Banking-Customers

"Too Many Crooks in the Kitchen" (September 4, 2015)

Is this the exploit kit equivalent of a clown car? Proofpoint researchers detect and analyze a single infection chain dropping a dozen payloads, including two separate pieces of ransomware.
Threats analyzed: Angler EK, Ransomware, Malvertising, Magnitude Exploit Kit (EK)
https://www.proofpoint.com/us/threat-insight/post/Too-Many-Crooks-in-the-Kitchen

“In Pursuit of Optical Fibers and Troop Intel: Targeted Attack Distributes PlugX in Russia” (September 15, 2015)

> Look inside a highly targeted campaign that uses specially crafted URLs and social engineering to spread the PlugX Trojan to targets in the Russian military and telco sectors
> *Threats analyzed:* PlugX Trojan, APT, Targeted Attacks, Phishing, Malicious URLs
> http://www.proofpoint.com/us/threat-insight/post/PlugX-in-Russia

“Operation Arid Viper Slithers Back into View” (September 18, 2015)

> Proofpoint researchers’ analysis of an update to Operation Arid Viper demonstrates that this threat still has teeth.
> *Threats analyzed:* Operation Arid Viper, Targeted Attacks, APT, Phishing
> https://www.proofpoint.com/us/threat-insight/post/Operation-Arid-Viper-Slithers-Back-Into-View

“Meet GreenDispenser: A new breed of ATM malware” (September 24, 2015)

> First analysis of a new variety of ATM malware that uses novel techniques to give attackers the ability to drain infected ATMs of their cash.
> *Threats analyzed:* Banking fraud, ATM malware
> http://www.proofpoint.com/us/threat-insight/post/Meet-GreenDispenser

“Dyreza Campaigners Set Sights on the Fulfillment and Warehousing Industry” (September 28, 2015)

> The infamous “man-in-the-browser” (MITB) banking malware Dyreza significantly expands its target set of entities from which to steal credentials.
> *Threats analyzed:* Dyreza/Dyre, Banking Trojans, MITB Attacks, Phishing, Credential Theft
> https://www.proofpoint.com/us/threat-insight/post/Dyreza-Campaigners-Sights-On-Fulfillment-Warehousing-Industry

about proofpoint
Proofpoint Inc. (NASDAQ:PFPT) is a leading security-as-a-service provider that focuses on cloud-based solutions for threat protection, compliance, archiving & governance, and secure communications. Organizations around the world depend on Proofpoint’s expertise, patented technologies and on-demand delivery system to protect against phishing, malware and spam, safeguard privacy, encrypt sensitive information, and archive and govern messages and critical enterprise information.

proofpoint™

892 Ross Drive
Sunnyvale, CA 94089

1.408.517.4710
www.proofpoint.com