FireEye
SECURITY REIMAGINED

SPECIAL REPORT

FIREEYE THREAT INTELLIGENCE

PINPOINTING TARGETS:

Exploiting Web Analytics to Ensnare Victims

NOVEMBER 2015

SECURITY REIMAGINED

CONTENTS

FIREEYE THREAT INTELLIGENCE
Jonathan Wrolstad
Barry Vengerik

INTRODUCTION

OVER THE PAST YEAR,

The individuals behind this activity have amassed vast amounts of information on web traffic and visitors to more than 100 websites—sites that the threat actors have selectively compromised to gain access to their collective audience.

we have identified suspected nation-state sponsored cyber actors engaged in a large-scale reconnaissance effort. This effort uses web analytics—the technologies to collect, analyze, and report data from the web—on compromised websites to passively collect information from website visitors.[1] The individuals behind this activity have amassed vast amounts of information on web traffic and visitors to over 100 websites—sites that the threat actors have selectively compromised to gain access to their collective audience.

Web analytics is used every day in much the same way by advertisers, marketers and retailers for insight into the most effective ways to reach their customers and target audiences. This paper explores the dark side of web analytics by demonstrating how the same tools and methods that fuel effective content delivery and e-commerce can potentially allow malicious actors to identify and target victims with pinpoint precision.

[1] Kaspersky Labs, Symantec and iSIGHT Partners have reported on campaigns similar, and possibly related to, the activity we describe in this report.

EVERY DAY, EACH OF US VISITS THE WEB AND NAVIGATES TO OUR FAVORITE SITES.

We accept that organizations routinely track our online activity. Companies monitor our clicks to see what links we are drawn to and how much time we spend on a given page. Marketers track our demographic information to better understand us as customers. Advertising firms generate revenue through referrals as we start our journey on one website and click a sponsored link to another. Shopping sites use cookies so that the shirt we viewed on a shopping website weeks ago shows up in an advertisement on our favorite news website. Organizations also learn about our computer systems. Scripts working in the background identify the type of browser, operating system or mobile device we are using so that the website displays properly. However, few of us are aware that cyber threat actors may be using those same tools to identify and target their next victims.

KEY FINDINGS




Threat actors use web analytics and open source tools to collect information about desired victims and their computers to track, profile, and possibly infect them with targeted malware.

The perpetrators alter specific websites to redirect visitors to a profiling script we call WITCHCOVEN. This script collects detailed information about the user's computer and installs a persistent tracking tool, called a "supercookie," which becomes part of a unique "browser fingerprint" that can identify the user's computer moving forward.

We believe the actors analyze the collected data to identify unique users and pair them with information about their computer to later deploy exploits tailored to their particular software and computer configuration.

The operation is most likely the work of threat actors aligned with a government based on the extensive collection of data, the culprits' operational restraint, and our assessment of their probable targets.

THE OPERATION

Beginning last year, we identified cyber actors integrating free, publicly available tools with custom scripts to monitor the online activities of Internet users without their knowledge,[2] just as corporations track the online activity of web users around the world. We believe these cyber threat actors are building profiles of potential victims and learning about the vulnerabilities in users' computers. These very same technologies that marketing firms use to track their clients and ensure their websites work on different types of web browsers can help cyber threat actors better identify their victims and tailor future infection attempts.

The cyber threat actors start by compromising large numbers of legitimate websites. The websites are not randomly chosen targets of opportunity, but specifically selected as part of a tactic called a strategic web compromise.[3] The attackers then modify the underlying HTML code on the website's home page (and often several subpages). This modification silently redirects visitors to a second website that has also been compromised to host a profiling script that we call WITCHCOVEN. WITCHCOVEN executes in the background without the user's knowledge, capturing the visitor's computer and browser configuration (see Figure 1 for more detail) and placing a highly persistent tracking cookie (a "supercookie") on their computer. In all, we identified over 100 compromised websites redirecting visitors to more than a dozen WITCHCOVEN profiling servers.

When an unsuspecting user visits any of the over 100 compromised websites, a small piece of inserted code—embedded in the site's HTML and invisible to casual visitors—quietly redirects the user's browser to a second compromised website without the user's knowledge. This second website hosts the WITCHCOVEN script,[4] which uses profiling techniques to collect technical information on the user's computer. As of early November 2015, we identified a total of 14 websites hosting the WITCHCOVEN profiling script.

We believe these cyber threat actors are building profiles of potential victims and learning about the vulnerabilities in users' computers.

The script provides the perpetrators with data on certain applications installed on the user's computer. WITCHCOVEN uses a number of open source web tools to retrieve this information such as the software version. These web tools are freely available, and website designers commonly use these (or similar) tools to enhance a users' browsing experience. For example, a site may routinely collect information about the type and version of visitors' web browsers to ensure that the site content displays correctly for as many visitors as possible.

The following are examples of some of the web tools embedded in the WITCHCOVEN code and the data they collect:

The "detect Office" module from the Browser Exploitation Framework,[5] an open source penetration testing tool, determines the Microsoft Office version on a computer by testing the browser's response to various ActiveX objects.

PluginDetect[6] is a JavaScript-based web tool to detect the type and version of various web-browser plugins, such as Java, Flash, Reader, and Shockwave.

[2] We detected a component of the process—the WITCHCOVEN profiling script—discussed later in the report.
[3] A strategic web compromise (SWC), also known as a "watering hole" attack, is a method of passively ensnaring victims as opposed to conducting an active attack such as a spear-phishing campaign. In an SWC, threat actors place exploit code on legitimate websites they anticipate their desired victims will visit as part of their normal online activity. If a targeted user travels to the compromised website with a vulnerable computer, malware can be installed on their machine.
[4] Technical details on the WITCHCOVEN profiling script are available in the appendix.
[5] https://github.com/beefproject/beef/tree/master/modules/browser/detect_office
[6] http://www.pinlady.net/PluginDetect/

WITCHCOVEN IN ACTION – PROFILING COMPUTERS AND TRACKING USERS

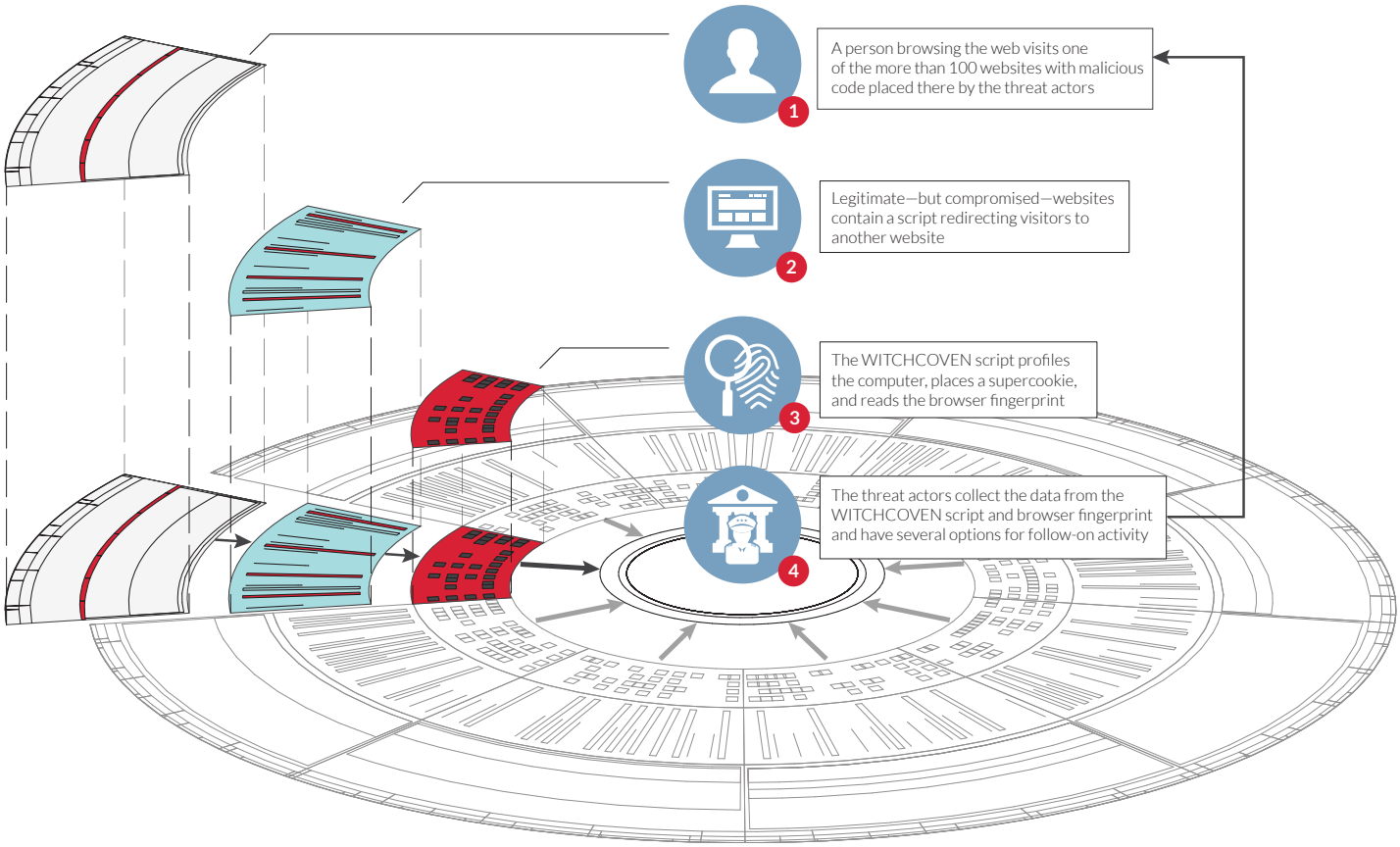
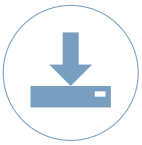


Figure 1 Strategic web compromise redirecting to WITCHCOVEN profiling script

In addition to collecting data about installed applications, browser plugins and their versions, the WITCHCOVEN script uses another open source tool known as "evercookie". evercookie is designed to create "extremely persistent cookies" on a user's computer by:



creating cookies in multiple storage locations on the computer

recreating deleted cookies, as long as any one cookie remains intact on the computer

attempting to propagate evercookies between browsers on the same computer

For these reasons, evercookies may be referred to as "supercookies" (because they use a broad range of storage mechanisms) or "zombie cookies" (because they may be recreated after deletion). In short, the evercookie provides a way to consistently identify and track a specific website visitor and is nearly impossible for the average user to remove. The evercookie and the other data gathered by the WITCHCOVEN script are sent back to the compromised web server using an HTTP POST request.

COOKIES, THIRD-PARTY COOKIES, AND SUPERCOOKIES

A website often uses HTTP cookies to track a visitor's actions on that site. For example, a news website might track the user's regional preference and an e-commerce site might track items in a visitor's shopping cart while they continue to browse other goods. Normal HTTP cookies are used by a single website and typically enhance a user's experience on the web.

Third-party cookies are HTTP cookies that can be set and read by third-party providers (such as ad companies or analytics services) that place content on other websites. Because these third-party providers host content across multiple websites, their cookies can track users across those sites. A provider who hosts content on a sports site and a shopping site can tell if the same user visits both sites based on data (such as unique identifier) within the third-party cookie. Over time, by noting the types of sites the user visits, these companies could build a demographic profile of the user (age, income, geographical location, interests), even if the user's identity is not known. While these cookies are not inherently malicious, some users view them as a privacy concern.

Both regular cookies and third-party cookies are typically stored in the user's web browser; modern browsers can be configured to periodically delete cached cookies or block certain types of cookies altogether. A "supercookie" refers to a cookie that uses alternate methods for storage, such as Flash cookies. In most cases, these cookies are not deleted by clearing the browser cache, making them much harder to find and remove. A supercookie—with its unique identifier—can therefore be used to persistently track and identify a particular user over time, even if the user attempts to block or delete cookies.

[7] https://github.com/samyk/evercookie

A MEANS TO A SINISTER END?

Although the WITCHCOVEN profiling activity may seem insidious or intrusive, so far nothing we have described is overtly malicious. No exploit code has been delivered. No website visitors have been compromised. As we noted above, these types of profiling and tracking techniques have legitimate purposes to optimize user experience and support marketing, demographic and sales analysis. So why did this particular activity capture our attention?

First, while many sites engage in profiling and tracking for legitimate purposes, those activities are typically conducted using normal third-party browser-based cookies and commercial ad services and analytics tools. In this case, while the individuals behind the activity used publicly available tools, those tools had very specific purposes. Using evercookie in particular implies that the actors wanted to ensure that visitors could be identified and tracked persistently over time, without having to worry about users enabling private browsing or deleting persistent cookies. This goes beyond "normal" web analytics.

Second, the legitimate websites that redirected visitors to the WITCHCOVEN script were themselves compromised. This was not part of a generic marketing campaign or routine web traffic analysis; someone deliberately and surreptitiously placed the redirect code on more than 100 compromised websites to profile visitors to those sites.

Finally—as we discuss below—while the redirect code was widespread, the compromised websites themselves were not arbitrary, but fell into an overall pattern. This led us to believe that the activity was not random, but targeted, and targeted at a specific set of users for what we believe is a unique purpose.

These observations led us to ask the questions: Why would someone be gathering this particular data in this manner? What could be the purpose behind this activity?

We believe that the computer profiling data gathered by the WITCHCOVEN script, combined with the evercookie that persistently identifies a unique user, can— when combined with basic browser data available from HTTP logs—be used by cyber threat actors to identify users of interest and narrowly target those individuals with exploits specifically tailored to vulnerabilities in their computer system.

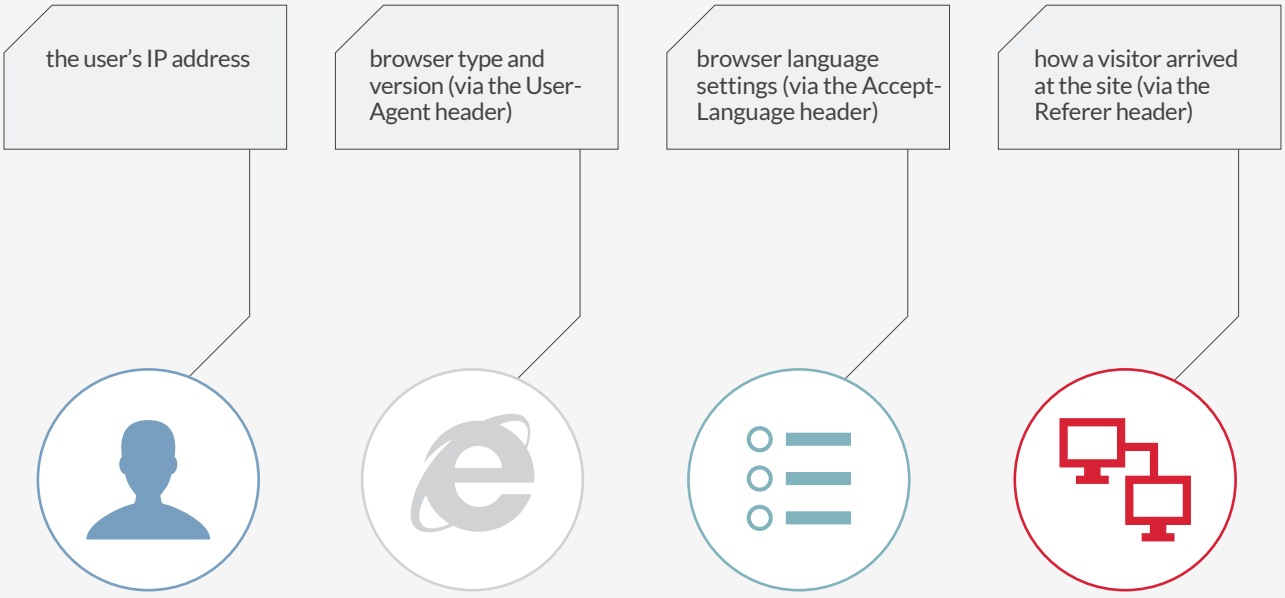
Why would someone be gathering this particular data in this manner? What could be the purpose behind this activity?

ASSEMBLING THE PIECES

How could mostly innocuous information-gathering lead to insidious, personalized attacks? Consider the implications of the data available to the WITCHCOVEN threat actors.

In addition to the data explicitly collected by WITCHCOVEN itself, the threat actors behind this activity would also have access to additional data about the user's browser, captured as part of normal web traffic in the HTTP logs of the compromised server hosting the WITCHCOVEN script. This data would likely contain, at minimum,[8] standard information such as:

...the threat actors behind this activity would also have access to additional data about the user's browser, captured as part of normal web traffic in the HTTP logs of the compromised server hosting the WITCHCOVEN script.



[8] Extensive research has been conducted on "browser fingerprinting"—using data available from a user's web browser to uniquely identify individual users. While we have no indication that the individuals behind WITCHCOVEN are leveraging browser fingerprinting to the full extent possible, the research shows the extent to which "innocuous" browser data can be used to identify individuals with a high degree of accuracy. See, for example, the Electronic Frontier Foundation's "Panopticlick" website (https://panopticlick.eff.org/index.php) illustrating this issue, and their associated whitepaper (https://panopticlick.eff.org/browser-uniqueness.pdf).

Although we do not know for certain whether the threat actors are making use of the log data, the data would be readily available to them. If we summarize the data available to the attackers (see Table 1), we see how they could build up a profile of potential victims. The threat actors could leverage the same data also used by legitimate businesses to perform web analytics to identify and profile users for potential malicious activity.

Table 1: Data available to threat actors and possible use

DATA	SOURCE	POSSIBLE USE
Version of Microsoft Office	WITCHCOVEN script	Identify older, unpatched, or vulnerable applications
Version of browser plugins (Java, Flash, etc.)	WITCHCOVEN script	Identify older, unpatched, or vulnerable applications
evercookie unique identifier	evercookie (WITCHCOVEN script)	Identify specific "user" (even if identity not known)
evercookie date	evercookie (WITCHCOVEN script)	Date/time of first visit to any of the compromised sites; timestamp can be correlated with HTTP logs to identify visitor IP address
Referring website	WITCHCOVEN script and HTTP logs	May help further identify or refine victim profile
IP address	HTTP logs	Source network of potential victim; may identify a particular corporation or organization of interest
Browser type / version	HTTP logs	Identify older, unpatched, or vulnerable browsers; identify browser with which another exploit (such as a Flash exploit) must be compatible
User's language	HTTP logs	May help further identify or refine victim profile

FINDING A NEEDLE IN A PILE OF NEEDLES

While the information above is potentially quite revealing about an individual user, it represents just one profile of one random visitor to one website. The threat actors behind WITCHCOVEN compromised more than 100 websites, each of which might have thousands of unique visitors each day. If, as we suspect, the culprits intended to use the data to target specific victims, they would need some means to analyze all of the data collected by the WITCHCOVEN profiling script (and presumably the web server log files) to identify specific targets for follow-on cyber operations.

We do not know exactly how the threat actors are using or processing the data. However, given the amount of data they have presumably collected in a year of activity, it is likely that they would need to use a large-scale data management and analysis system. At a minimum, this would involve a database of potential targets; it may also involve performing web analytics on the collected data to help identify targets of interest. To do this, they may use web analytics tools such as a customer relationship management (CRM) database just as many legitimate companies do. A CRM allows businesses to track sales, customer interactions, and online marketing campaigns. The threat actors behind this activity could mine the collected data based on their targeting criteria, searching for potential victims. The refinement process might look something like this:

1	Determine whether desired types of victims are visiting the compromised sites
2	Determine what other sites desired victims are visiting (to find possible new collection points)
3	Identify specific victims

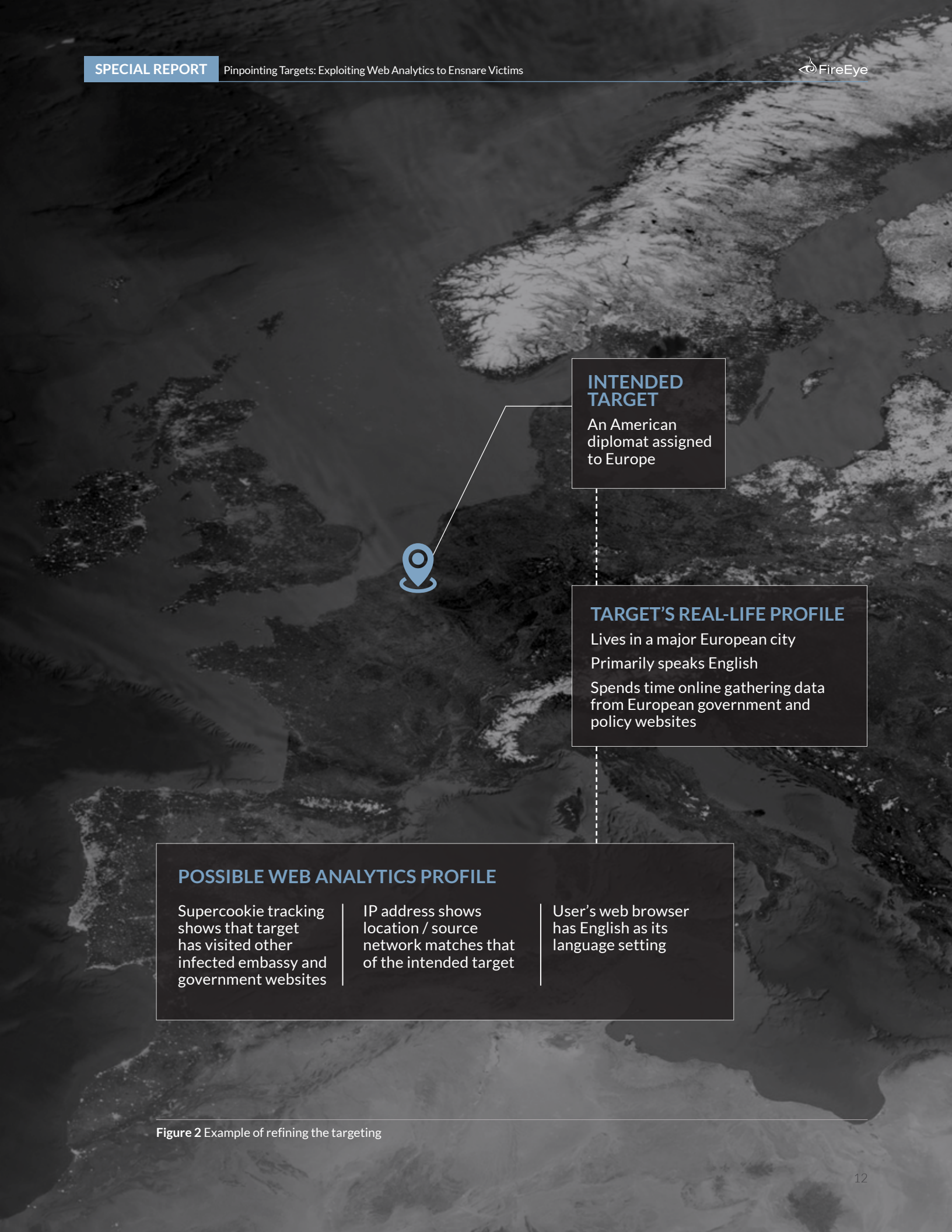


Figure 2 Example of refining the targeting

EMPLOY THE DATA TO DELIVER MALWARE

Once specific targets have been identified from the collected information, we believe the actors behind this operation could design and deploy highly tailored exploits to increase the chances of compromising specific targets. We have not yet observed any follow-on exploitation within our customer base; however, it could be that the threat actors' targeting is so narrow and highly focused that the odds of observing an exploit and malware payload delivered to an individual victim are extremely low.

Despite the lack of confirmed follow-on activity, the information the threat actors collect could be used to deploy custom exploits tailored to a victim's specific vulnerabilities as identified in the WITCHCOVEN profiling and designed to deliver malware to the victim's computer. For example:

The perpetrators might note that a user is running an outdated version of Adobe Flash, known to be vulnerable to particular exploits. The ability to target older, known (but unpatched) vulnerabilities means the actors would not have to risk use and exposure of more valuable exploits, such as a zero-day exploit.

The discovery of outdated software versions might also provide insights into the general security practices of the potential victim, affecting the group's choices for follow-on activity or the use of particular malware. The actors could use standard backdoors against victims with only moderate defenses, saving sophisticated backdoors for more vigilant environments.

If the user is running fully patched computer software, existing exploits will be ineffective and the group will need to develop, procure, or deploy a zero-day exploit. This knowledge would allow the group to limit the use of zero-day exploits to a small group of high-value targets.

USING VICTIM PROFILING TO SMARTLY TAILOR TARGETED OPERATIONS

The threat actors behind the activity discussed in this report appear to use an even more narrowly scoped approach to choose victims than we have previously observed. Other cyber threat groups have also used scripts or other server-side code to profile potential victims and narrowly deliver tailored exploits. For example, cyber criminals have created websites that contain code that delivers malware only to specific site visitors, such as those from a particular geographical region (based on IP address) or to every 10th visitor (to limit exposure of the malicious activity).

Some of the skilled nation-state threat groups we track use similar profiling scripts to ensure effective delivery of exploits and their associated payloads.

- As part of Operation Clandestine Wolf,[9] the Chinese advanced persistent threat (APT) group APT3 used a profiling script before deploying a Flash zero-day exploit.
- During Operation Russian Doll,[10] the culprits, suspected to be the Russian group APT28, collected information about potential victim systems before deploying two zero-day exploits.

In these cases, the profiling scripts only delivered the exploit code to computers that were actually vulnerable. This technique increases the likelihood of success, reduces exposure to security researchers because only a few victims receive the exploit and likely delays the discovery of the attackers' valuable zero-day vulnerabilities.

[9] Eng, Erica and Dan Caselden. FireEye. "Operation Clandestine Wolf – Adobe Flash Zero-Day in APT3 Phishing Campaign." 23 June 2015. https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html

[10] FireEye Labs. FireEye. "Operation RussianDoll: Adobe & Windows Zero-Day Exploits Likely Leveraged by Russia's APT28 in Highly-Targeted Attack." 18 April 2015. https://www.fireeye.com/blog/threat-research/2015/04/probable_apt28_useo.html

COLLECTED DATA: HOW IT COULD BE USED

FOLLOW-ON CUSTOM EXPLOITATION

Once the cyber threat actors have identified their victims and the exploits likely to be successful, they could deploy an additional script that runs after the WITCHCOVEN profiling script and is designed to compromise a specific victim. As a simple example, this script could check the unique identifier in the evercookie of a site visitor and deliver a specific exploit only if the identifier matches a target list. The next time a targeted user browses that website, the script's logic would be triggered and an exploit would be sent to the user's computer. Limiting the delivery to only chosen victims would decrease the likelihood of attracting the attention of security researchers and of the exploit script being noticed on the web server.

SPEAR PHISHING

The use of supercookies and browser fingerprints can track, profile and possibly identify individual users based on unique identifiers. If the perpetrators were able to use additional data to link the identifier to an individual, they could use the information gathered to create a well-crafted spear-phishing email with an attachment designed to appeal directly to very specific details of the target's interests. The attachment could be weaponized with an exploit explicitly chosen to compromise the victim's computer configuration, greatly enhancing the likelihood of a successful infection.

HUMAN INTELLIGENCE OPERATIONS

The sponsor of this reconnaissance could use the collected information to build a profile to assist in targeting an individual for traditional spying.

CREATION OF A DATABASE OF TARGETS

APT actors have shown an interest in supporting their intelligence collection goals by amassing large amounts of personal data, most likely to create databases to keep track of current and future targets of interest. The threat actors could use the data collected to create a rich database of potential targets and their associated computers.

Figure 3 Potential uses for the collected data

EFFECTIVE, EFFICIENT AND STEALTHY

This activity most likely is the work of a state-sponsored group that aims to collect global reconnaissance data to enable future cyber operations.

We assess this activity most likely is the work of a state-sponsored group that aims to collect global reconnaissance data to enable future cyber operations. Our assessment is based on:

SCOPE OF OPERATIONS	The operation collects information from compromised websites around the globe. Data collection on this scale likely requires ample resources to analyze the information and identify targets. The scale of this activity also implies that the threat actors are seeking data to satisfy a sizeable list of intelligence requirements, typical only of a large nation state.
OPERATIONAL RESTRAINT	Strategic web compromises are not uncommon; the unusual part of this operation is the lack of any obvious exploit or malware delivery. If the threat actors are using the collected data for pinpoint targeting, as we surmise, this implies a group that wants to limit exposure of its tools and maintain a high degree of operational security—both of which suggest this is a long-term operation to fulfill specific intelligence requirements.
PROBABLE TARGETS	Based on the set of compromised websites, the threat actors target individuals who may be of high interest to a government collecting intelligence.

As previously noted, we identified more than 100 compromised websites hosting the redirect to the WITCHCOVEN profiling script. When viewed as a whole, the sites were not random; they focused on a diverse but relatively narrow set of interests. The compromised websites would attract visitors involved in international travel, diplomacy, energy production and policy, and international economics, as well as those serving in foreign governments—all individuals that would likely have information pertinent to a state's strategic interests (see Figure 4 for the industry breakdown of compromised websites).

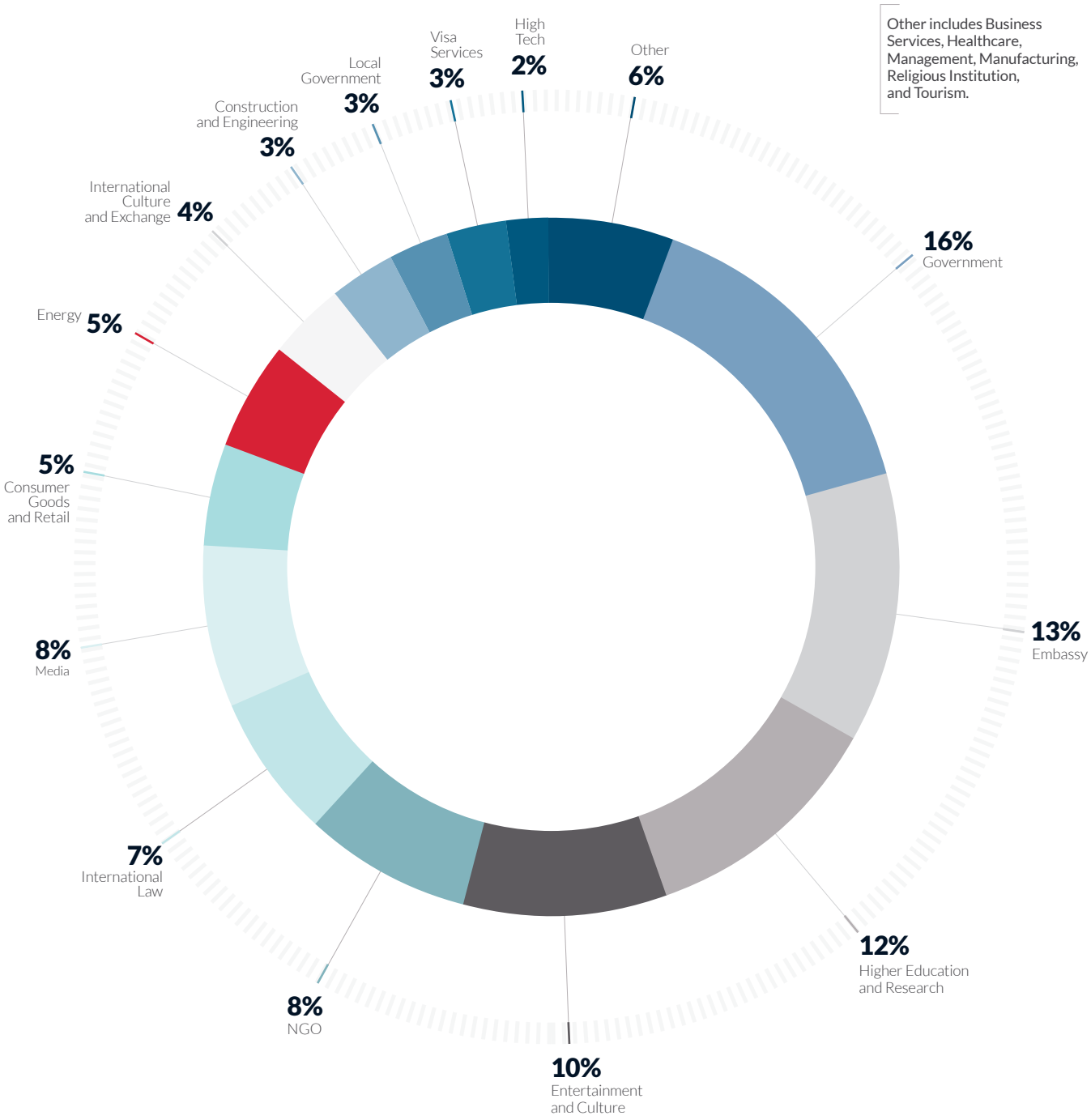
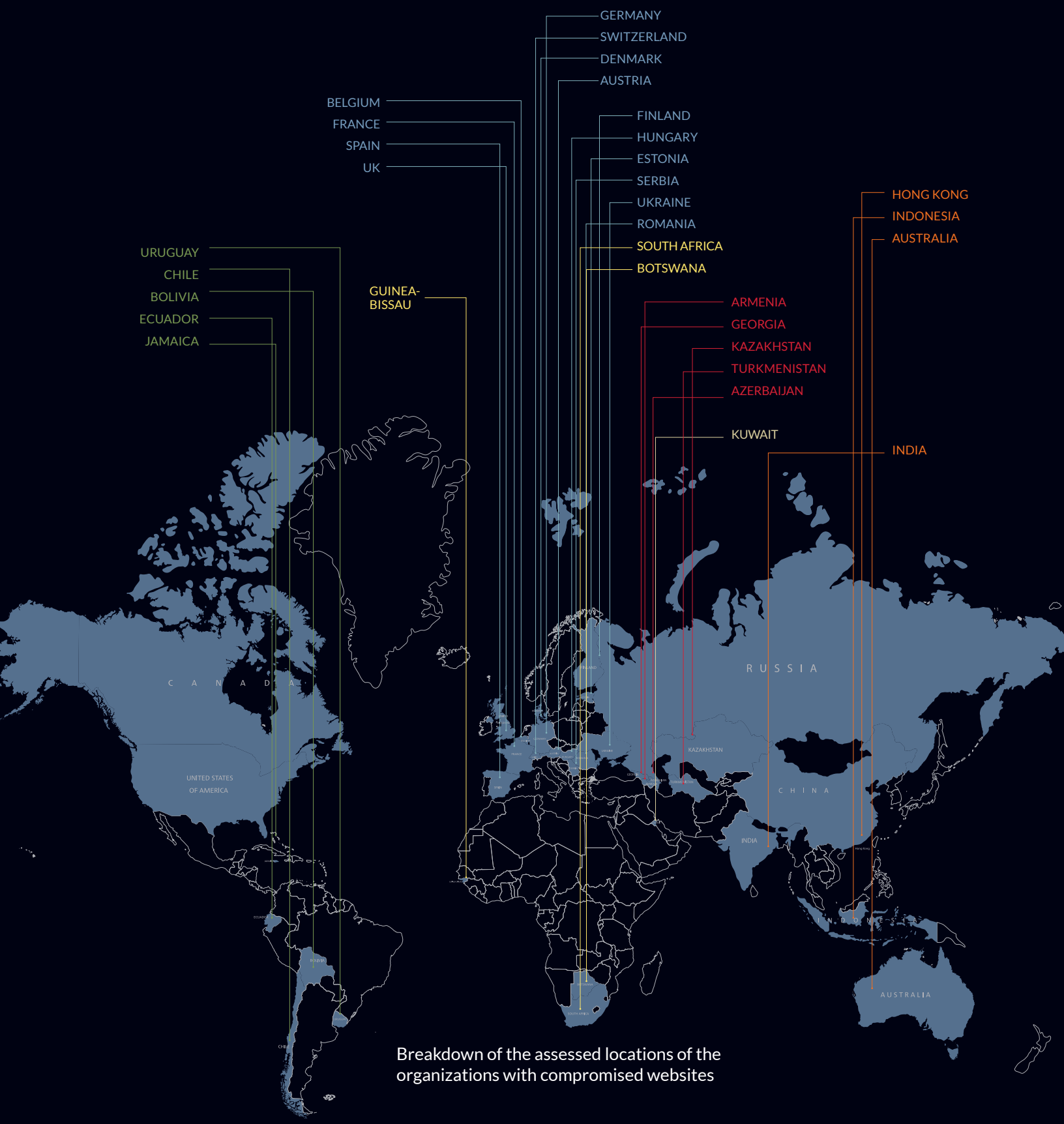


Figure 4 Breakdown of compromised websites hosting the redirect to WITCHCOVEN script by industry as of Nov. 1, 2015

	Government	16%		International Law	7%		Construction and Engineering	3%
	Embassy	13%		Media	8%		Local Government	3%
	Higher Education and Research	12%		Consumer Goods and Retail	5%		Visa Services	3%
	Entertainment and Culture	10%		Energy Company	5%		High Tech	2%
	NGO	8%		International Culture and Exchange	4%		Other	6%



Breakdown of the assessed locations of the organizations with compromised websites

LIKELY INTENDED TARGETS:
Government Officials and Executives in the U.S. and Europe

We believe the compromised websites indicate the threat actors are especially interested in collecting data from executives, diplomats, government officials and military personnel, particularly those in the U.S. and Europe. The compromised websites include visa services firms and certain embassies in the United States, which may attract U.S. government officials or executives traveling to Russia, the Middle East and Africa. The compromised sites in Europe probably attract Internet users interested in European politics, diplomacy, research institutes and business ties between Europe and the United States. In addition, compromised sites indicate the actors' interest in targeting individuals who work in the energy discovery, production, and technology industries, particularly those involved in natural gas extraction and other energy-related activities. Based on the focus of other compromised sites, additional individuals of interest might include:

- Diplomats and business people in the United States and Spain, as well as Vienna and Brussels, the headquarters of many global intergovernmental institutions
- Individuals involved in issues of energy policy and climate change, particularly energy research and consulting organizations
- Latin American government officials
- European economists
- Individuals and organizations with a nexus to Ukraine or the Republic of Georgia

Focus on Eastern Europe and Russian Organizations

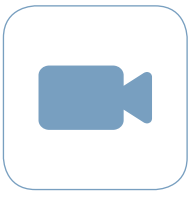
Finally, other websites hosting the redirect suggest that those behind this activity may have an interest in individuals with a nexus to:

a major Russian energy company

Russian cultural organizations and information resources

a Russian embassy website

Ukraine's security services and border guards



a media organization operating in the Republic of Georgia

Similar Reporting

Kaspersky Labs, Symantec, and iSIGHT Partners have all reported on widespread campaigns similar to the activity we describe in this report. In August 2014 Kaspersky described the "Epic Turla" operation,[11] while in January 2015 Symantec reported on the "Waterbug" campaign.[12] Both operations combined strategic web compromises (SWCs) with profiling scripts and malware delivery.[13] iSIGHT's findings in the spring of 2015[14] characterized an SWC operation whose targeting directly overlaps with the WITCHCOVEN activity described in this paper.

Collateral Damage: Snaring Unintended Victims

Common themes among compromised websites suggest the culprits are interested in targeting specific types of individuals. However, detections of the WITCHCOVEN profiling script among our customers demonstrate there is a more widespread effect. SWCs often leave a wake of collateral damage, and the culprits inadvertently snare unintended victims who happen to navigate to their sites.

We have detected alerts for WITCHCOVEN from customer organizations in nearly all industries.[15] Education, government, financial services, energy, and the entertainment industries appear to be the most affected. Figure 5 depicts the share of detection alerts for WITCHCOVEN among FireEye customers by industry from March 18 to Oct. 31, 2015.

We have detected alerts for WITCHCOVEN **from customer organizations in nearly all industries.**

[11] Kaspersky Labs. "The Epic Turla Operation: Solving some of the mysteries of Snake/Uroburos. 7 Aug 2014. https://securelist.com/analysis/publications/65545/the-epic-turla-operation/. Accessed 28 Oct 2015.
[12] Symantec. The Waterbug Attack Group. 16 Jan 2015. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/waterbug-attack-group.pdf. Accessed 16 Sep 2015.
[13] The malware was identified as Wipbot and Turla, both suspected of being used by Russian state-sponsored threat actors.
[14] Gertz, Bill. "State report reveals 130 compromised websites used in travel-related watering hole attacks." Flash//Critic. 4 April 2015. http://flashcritic.com/state-report-reveal-130-websites-used-travel-related-watering-hole-attacks/. Accessed 15 September 2015.
[15] These statistics are from FireEye customers who have opted to share anonymized data with FireEye. The data included in the FireEye Dynamic Threat Intelligence (DTI) platform allows the firm to gain insights into cyber threat activity by gathering real-time information about the latest cyber threats worldwide. DTI uses millions of FireEye sensors to perform more than 50 billion analyses over 400,000 unique malware samples every day.

BREAKDOWN OF ALERTS BY INDUSTRY

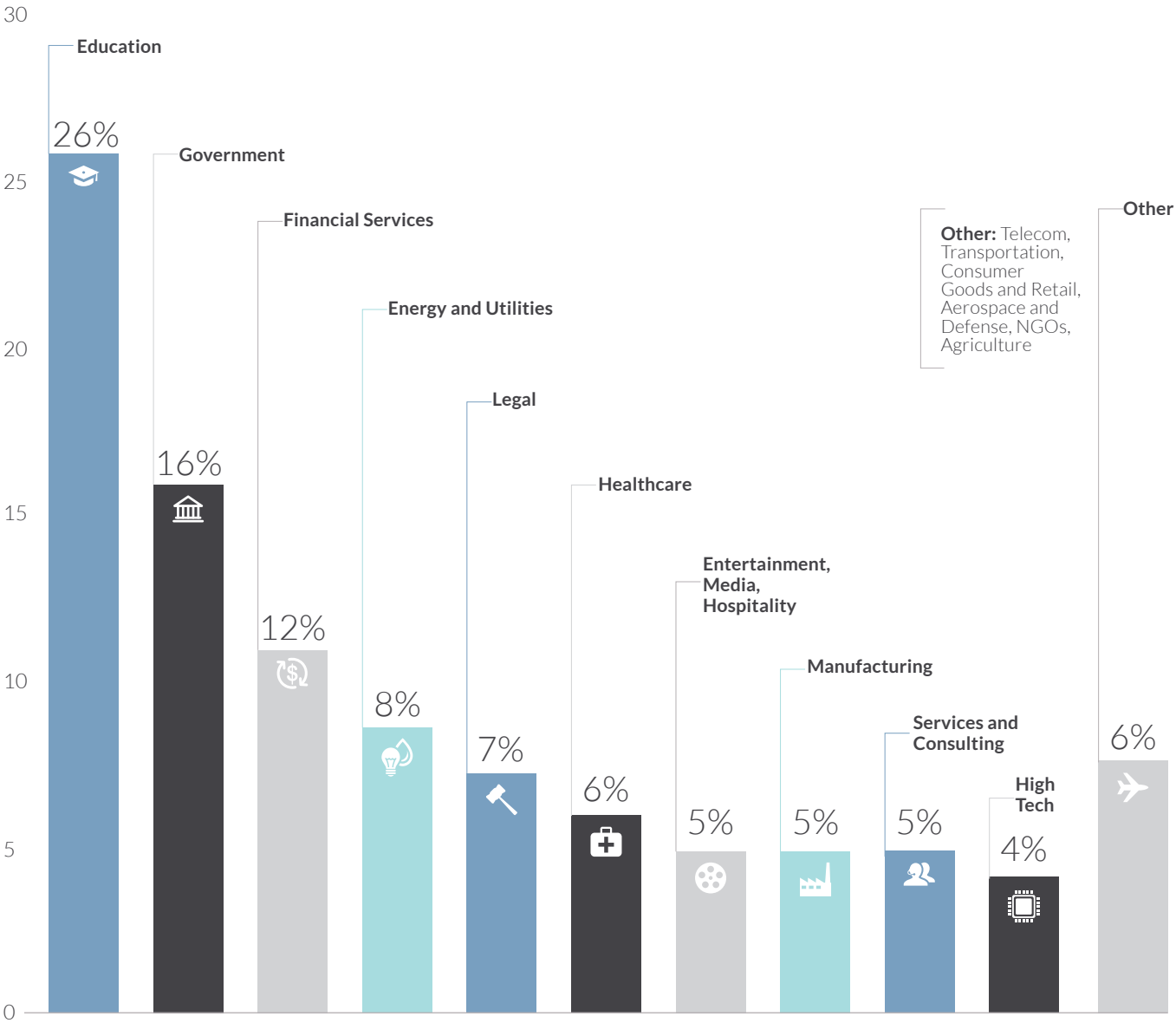


Figure 5 FireEye customers, broken down by industry, that were alerted on the WITCHCOVEN profiling script between March 18 and Oct. 31, 2015

MITIGATION

Customers often ask for ways to mitigate the risk against the malicious cyber activity we observe. For the activity described in this report, mitigation is a challenge because the threat actors are collecting information about potential targets in the course of a user's normal web browsing activity. The collection is done using similar scripts, tools and methods that legitimate websites use to profile customers and enhance the browsing experience.

While profiling may feel invasive, it does not compromise a victim's computer. Individuals and organizations can take steps such as blocking script execution or using third-party cookies, enabling privacy-enhanced browsing, or using anonymization services (such as the TOR browser) to help mask their identity. However, these measures may be burdensome to implement and, while blocking potentially malicious activity, may also prevent legitimate site content from loading.

Organizations may be better off focusing on detecting or preventing any follow-on attacks through best practices, including disabling unneeded plugins, ensuring that systems and applications are patched, and monitoring hosts and networks for suspicious traffic.

APPENDIX:
Technical Details

The WITCHCOVEN profiling script (example MD5: 634438A50AE1990C4F8636801C410460) is written in JavaScript. The script contains the jQuery JavaScript library that is obfuscated to remove variable names. The full script is quite lengthy but is largely comprised of identical or slightly modified versions of publicly available scripts, including evercookie, PluginDetect and the "detect Office" module from the Browser Exploitation Framework Project.

The script gathers the information listed in Table 1 and encodes it in a URL request to the compromised website hosting the WITCHCOVEN script.

Table 2: URL request variables

VARIABLE NAME	VARIABLE DATA
sid	Adobe Shockwave version
fid	Adobe Flash version
aid	Adobe Reader version
mid	Microsoft Office version
jaid	Oracle Java version
rid	HTTP Referer
cid	First date the evercookie supercookie was set (in epoch time), or the current date if the evercookie was never set
cart_id	55 (static value; may vary across WITCHCOVEN instances)

To download this or other
FireEye Threat Intelligence reports,

visit: https://www.fireeye.com/reports.html

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | **www.fireeye.com**