EXHIBIT 9

WHITE PAPER

Combatting Drive-By Downloads

A Next Generation Appoach to an Emerging Threat

CYPHORT™

Introduction

When was the last time you bought a cool gadget because you heard an advertisement for it on the radio, or a nice pair of jeans because you saw a commercial for it on the television? You're probably guilty of spending a few hours every month looking for something to buy on Amazon or any other online retailer. Thanks to its convenience, online shopping has become a major trend over the last few years and lets face it, it's here to stay. With the rise of online shopping, marketing experts capitalized on this new avenue to advertise their products. Now your friends nudge you on Facebook to buy a product they love and Google suggests a friendly place across the street where you can get your car fixed. It's become hard to browse even a few pages without running into an ad and because of this increases, malware experts also saw a new avenue of attack - Malvertising.

Malvertising involves injecting malicious code into legitimate advertisements. These attacks started off as amateur "Click on Me!" buttons which fooled a lot of people. A popular example of this is a link that tricks the user into installing a fake Antivirus program which is actually a malware in disguise. However, over time with enough awareness and educating users not to give into the "Ooh, what does this button do?!" reaction, people became mindful of what they clicked and attackers had to become more sophisticated, paving the way for a new type of threat called "Drive-by Downloads". Drive-by download is a method that attackers use to automatically download a malware to the endpoint without a conscious user action such as clicking on a button or link.

Anatomy of a Drive-by Download

A drive-by download is a multi-stage attack:

1. The attacker embeds malicious code into an online advertisement displayed on a trusted website.
2. A user visiting the website gets redirected to the attacker's site without the user clicking on the advertisement.
3. An exploit kit from the attacker's site looks for possible vulnerabilities on the user's endpoint.
4. Based on the exploit discovered, a desired malware is downloaded to the endpoint without the user's knowledge.

A drive-by download is a sneaky attack where a user normally browsing a seemingly harmless site can get infected without clicking on anything. The benign website can be compromised in different ways - by embedding malicious code in a comment field on a blog or a poorly secured web form. But the easiest way to go about this is by taking advantage of a flaw in an online advertisement and injecting malicious code in it. Trusted websites that are visited by thousands every day can end up hosting advertisements running malicious code without their knowledge.

The malicious code injected into the advertisement redirects the user to the attacker's website by loading the malicious url in a new window. This new window goes undetected because attackers make use of a common HTML feature called Inline Frame or iFrame for short. An iFrame is an HTML document that is embedded into another HTML document. For example, a YouTube video can be seamlessly embedded into a main webpage. In reality, it is just a regular webpage playing a YouTube video that is inserted into the main page by adjusting the size and removing the borders, it gives an illusion that the YouTube video is actually a part of the main webpage. So when the malicious code redirects the user to a different website, it opens up in a tiny window which can't be easily spotted by the human eye.

Once the user gets redirected to the attacker's web page, an exploit kit examines the endpoint for possible vulnerabilities to take advantage of. This is the beginning of the attack. The exploit kit gathers information about the operating system, browser type, browser version and browser plugins and looks for security holes in them. Browser plugins such as Java Runtime Environment, Adobe Flash Player, Adobe Reader are popular targets. The exploit itself doesn't cause any actual damage - the security codes of the building have been cracked, but nothing has been stolen yet.

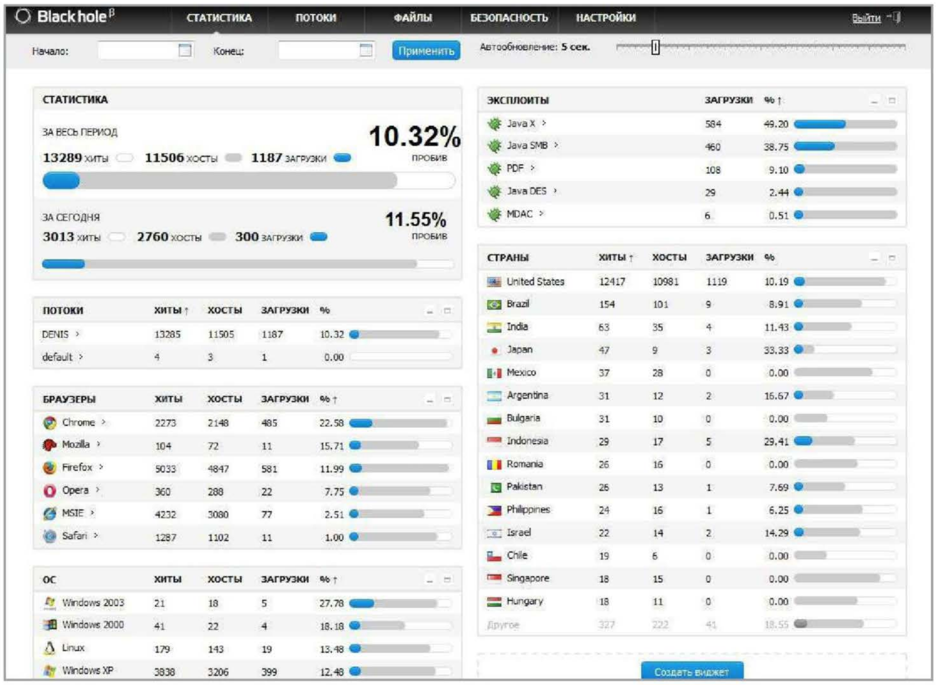
Armed with the knowledge of how to attack the victim, the exploit kit proceeds to download an appropriate malware to the victim's endpoint. The malware also known as "payload" is automatically installed on the endpoint without the user's knowledge. The payload download goes unnoticed because it is usually obfuscated. Obfuscation is a common technique used by attackers to evade traditional signature based detection engines and helps mask the real purpose of the malicious code. Once the malware has been downloaded and executed, it proceeds to do what it's best designed for - to make some green for the attacker. The malware can extract crucial banking information or lock your folders in exchange for money (more commonly known as Ransomware). Even more insidious attacks may start with reconnaissance tools that stay "low and slow" and take stock of critical assets on the network and sniff for access credentials.

Even for the well aware, with new vulnerabilities discovered every other day, it becomes tedious for a user to go through the ritual of updating the software - closing all applications that use the software, wait for the update to complete and then start all the applications back again.

Drive-By Downloads On the Rise

Drive-by downloads have become a serious threat and there are several reasons for this:

> One of the most compelling reasons is the fact that any person with a malicious intent and almost zero malware writing skills can stage a drive-by download attack on several endpoints across the world. Exploit kits and payloads are sold in the darknet or underground markets and it has become easy for an attacker to get hold of one. Since the darknets are anonymous, it is sufficiently harder to trace these purchases. Sophisticated hackers have also developed exploit kits that are easy to use. Modern exploit kits provide a graphical user interface to help the attacker decide who his next victims will be and also show the progression of infections on a victim's machine. It even has a fancy dashboard that shows statistics on the number of machines the attacker was able to infect that day. The attacker can sort all this data by OS, browser or country, and yes, they can even generate pie charts and graphs to organize the victim data. Some exploit kits have taken it to the next level by including multiple-user support and an authorization system to allow groups of users to manage their data.



Автообновление: **5 сек.**

СТАТИСТИКА

ЗА ВЕСЬ ПЕРИОД

13289 хиты **11506** хосты **1187** загрузки

10.32% пробив

ЗА СЕГОДНЯ

3013 хиты **2760** хосты **300** загрузки

11.55% пробив

ПОТОКИ	ХИТЫ ↑	ХОСТЫ	ЗАГРУЗКИ	%
DENIS ›	13285	11505	1187	10.32
default ›	4	3	1	0.00

БРАУЗЕРЫ	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	% ↑
Chrome ›	2273	2148	485	22.58
Mozilla ›	104	72	11	15.71
Firefox ›	5033	4847	581	11.99
Opera ›	360	288	22	7.75
MSIE ›	4232	3080	77	2.51
Safari ›	1287	1102	11	1.00

ОС	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	% ↑
Windows 2003	21	18	5	27.78
Windows 2000	41	22	4	18.18
Linux	179	143	19	13.48
Windows XP	3838	3206	399	12.48

ЭКСПЛОИТЫ	ЗАГРУЗКИ	% ↑
Java X ›	584	49.20
Java SMB ›	460	38.75
PDF ›	108	9.10
Java DES ›	29	2.44
MDAC ›	6	0.51

СТРАНЫ	ХИТЫ ↑	ХОСТЫ	ЗАГРУЗКИ	%
United States	12417	10981	1119	10.19
Brazil	154	101	9	8.91
India	63	35	4	11.43
Japan	47	9	3	33.33
Mexico	37	28	0	0.00
Argentina	31	12	2	16.67
Bulgaria	31	10	0	0.00
Indonesia	29	17	5	29.41
Romania	26	16	0	0.00
Pakistan	26	13	1	7.69
Philippines	24	16	1	6.25
Israel	22	14	2	14.29
Chile	19	6	0	0.00
Singapore	18	15	0	0.00
Hungary	18	11	0	0.00
Другое	327	222	41	18.55

The recent Angler exploit gives us some insight into how mature exploit kits have become. The developers of Angler Exploit Kit were always one step ahead in the game. Updates to the kit to exploit new vulnerabilities were faster than security updates to patch the targeted software. The Angler Exploit Kit could detect if an antivirus was installed on the endpoint or if it was being run in a sandbox.

Another reason for the increase in drive-by download attacks is the means by which hackers spread exploits. Planting drive-by downloads on trusted websites using vulnerabilities in online advertisements increased the proliferation of exploits by multiple folds. Cyphort Labs investigated the Angler Exploit Kit and discovered several infected domains spread across the United States, Italy, Germany, Japan, India and more. At least 10 million people visited those websites within a period of 10 days. One of the popular domains that was infected was The Huffington Post.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**

fastcase®
Smarter legal research.