

## DEKENEAS APT HUNTER

*“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. 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. The name is derived from predators in the natural world, who wait for an opportunity to attack their prey near watering holes.” ([https://en.wikipedia.org/wiki/Watering\\_hole\\_attack](https://en.wikipedia.org/wiki/Watering_hole_attack))*



### What is a watering hole?

Imagine yourself browsing your favorite website, or worse, browsing a website that you need to perform your daily tasks at your workplace. You trust the website, because you know it is a legitimate website, and you trust the antivirus product on your device, because you know your subscription is up to date. But still, somehow, **your device ends**

**up compromised.** You did not open that e-mail coming from a dubious e-mail address and you did not click on that link a suspicious looking user sent you on social media. Yet, somehow they managed to access your work e-mail, your documents, your social media profiles and your banking application. How did that happen? Quite possibly it happened through a *watering hole attack*.

Home > Security

 **SECURITY ADVISER**  
By Roger A. Grimes, Columnist, CSD | MAY 21, 2013 8:00 AM PT

**ANALYSIS**

### Watch out for waterhole attacks -- hackers' latest stealth weapon

It's time to learn about waterhole attacks, where sites with tailored malware await visits by certain companies' employees



The bane of the computer security world is how long it takes to recognize and respond to new attack paradigms. Name a major threat -- the boot virus, macro virus, email attachment, or Web JavaScript redirect -- and it seems to take years to respond adequately.

So here's an early warning: Waterholes should be on your radar.

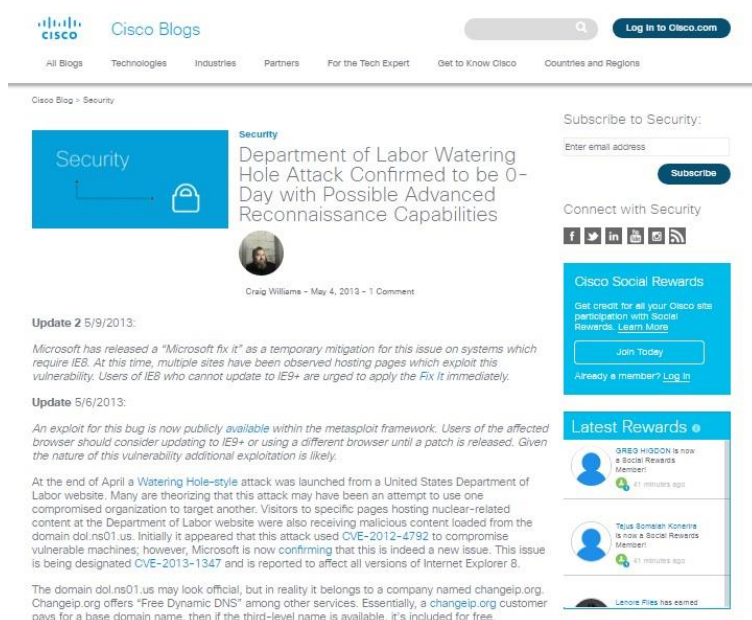
[ Brace yourself for [IT's 9 biggest security threats](#). | Find out how to [block the viruses, worms, and other malware that threaten your business](#). | Learn how to protect your systems with InfoWorld's [Security Central newsletter](#). ]

**MORE LIKE THIS**

-  Best new Windows 10 security features: The privacy edition
-  What is cryptojacking? How to prevent, detect, and recover from it
-  Your quick guide to malware types

Watering hole attacks are very stealthy and almost impossible to detect in due time, and **your antivirus cannot protect you**. Your fancy and expensive firewall cannot protect you either. Because they either need a *signature* or *specific malicious behavior* to be able to detect an attack. And watering hole attacks can be made to look in many ways, thanks to the inner specifics of HTML and HTTP protocols, thus they rarely share a common pattern. Apart from this, most of them use so-called *zero days* exploits, which are exploits unknown to the public at the moment of the attack, therefore there is no way to look for a signature. Another approach would be to analyze every page in every website you visit in a sandbox environment. But a sandbox needs at least a few tenths of seconds to analyze a page. And there are hundreds of websites, with hundreds of pages, visited every day on average in every organization. Plus, attackers using the “watering hole attack” technique have another trick in their bag

in order to defeat a selective attack. For instance, they can choose to attack only certain browser technologies and certain versions, or only web clients coming from certain IP addresses, or speaking a certain language, etc., leaving all






other users untouched. And they have means to fingerprint sandboxes, knowing that there is a trap and deciding not to attack. Therefore, a sandbox, or an analyst needs to guess what

technologies, IP addresses or other specifics the attackers target. And they need to apply evasion tricks which are not always feasible.

## How dangerous is the watering hole attack?

They are dangerous enough to have been used to compromise corporate networks of tech giants such as Google, Microsoft, Apple, Facebook, Twitter but also countless banks, telecom companies, government officials or investigative journalists. Due to its specifics and difficulty of detection, the watering hole attack is the preferred attack of today's cybercriminal and advanced persistent threat groups.

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

Author:  
Michael Mimosa  
February 02, 2017  
4:07 pm

A minute read

Share this article:

f t in



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.

 **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.

PRIVACY AND SECURITY

## Google Hackers Reveal Websites Hacked Thousands of iPhone Users Silently for Years



Dell Cameron  
8/30/19 1:00pm • Filed to: PROJECT ZERO

234.9K

69

5







## How does DEKENEAS protect against browser attacks (exploits, watering hole cryptojacking)?

DEKENEAS employs a proprietary technology first presented at DEFCAMP 2016 (<https://def.camp>), the largest Cyber Security Conference in Eastern Europe, based on complex artificial intelligence algorithms and it is able to “understand” a web page content without actually having to run it. Its unique feature set is able to accurately describe the maliciousness of each element inside the page, detecting *browser exploits*, *watering holes* or *cryptojacking attacks*. We were able to achieve this level of accuracy after

[illegible]

analyzing more than 40,000 malicious samples found in the wild, which we used to train

our algorithms. In the figure on the left there is an actual malicious script we found in the wild, linked to a campaign used to compromise iPhone users speaking a certain language. As you can see, it is virtually impossible for a traditional security solution to accurately pinpoint this malicious script, yet DEKENEAS managed to accurately find it due to its unique feature set which triggered this script as highly suspicious. But there is more... DEKENEAS has a unique engine which analyzes suspicious elements it finds and tries to further understand them: which technologies they target, if there are certain IP addresses who are targeted or other features to fingerprint and classify users and it uses this information to start proprietary sandboxes that emulate a real user that fits the profile targeted by the attackers, raising the chances of identifying ongoing attacks even if they are highly targeted.

## How can I use DEKENEAS?

In its simplest form, DEKENEAS can be used by *registering to the website* <https://www.dekeneas.com> and listing the websites you visit and specifying how often you want to scan them: daily, weekly or monthly. The website will generate a report as soon as the scan is finished. Also, you can use DEKENEAS *through an API*, integrating it directly with your firewall. Using this approach you benefit of a *threat intelligence feed* custom tailored to your needs. If you do not have a firewall or proxy system you can integrate with DEKENEAS, we offer you *DEKENEAS WSG appliances* which are either virtual or physical web proxies integrated with DEKENEAS engine. Or you could simply *subscribe to our threat intelligence feed*, which will not be custom tailored to your needs but will contain malicious websites we found during our regular scans.



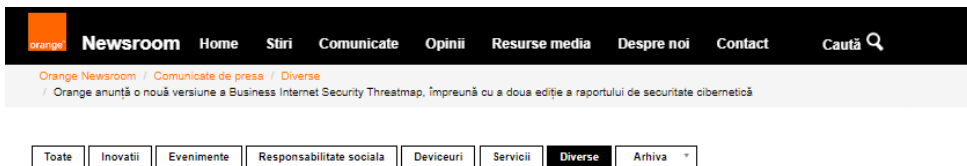
## WHO IS USING DEKENEAS?

Starting with October 2018 Dekeneas became part of ORANGE start-up acceleration initiative “ORANGE Fab”, and also has been integrated in Business Internet Security Threatmap which is an ORANGE initiative to “draw” the map of Internet threats targeting ORANGE customers. Also, a sum of banks both local and from abroad, governmental institutions and other customers from various industries, from financial to automotive



and mass-media, chose to use DEKENEAS APT HUNTER in order to protect themselves against the insidious threats posed by watering holes, browser exploits or cryptojacking attacks, generating a 300% growth in the first year of activity.

Ioan Constantin, Cyber Security Expert, Orange Romania: *“I had the opportunity to work closely with Dekeneas from the early iterations up to the current versions and witness how an ambitious project stemming from a cyber security startup actually accomplishes a coherent transformation to a fully-fledged, mature and reliable early detection system that is able to detect with pin-point precision, emerging threats that challenge today’s defensive technology. In the past 2 years of collaborating with Dekeneas we managed to integrate their APT Hunting and code analysis technologies in products and services that will offer dependable protection and enhanced visibility to our B2B customers and we’re pushing forward on integrating new features, new detection capabilities and intelligence capabilities to what is – in my opinion – a winning solution. I’m confident that Dekeneas is and continues to be a stop-gap solution to today’s and tomorrow’s cyber security challenges.”*



## Orange anunță o nouă versiune a Business Internet Security Threatmap, împreună cu a doua ediție a raportului de securitate cibernetică

11.10.2019 Orange România lansează o nouă versiune a Business Internet Security Threatmap (BIS Threatmap), un instrument gratuit menit să crească nivelul de conștientizare în ceea ce privește securitatea cibernetică a companiilor și autorităților locale.

Lansată în 2017, platforma colectează în timp real date prin soluția Business Internet Security. Această soluție analizează peste 5 milioane de amenințări pe lună în infrastructura de securitate a clienților business Orange. BIS Threatmap agregă datele anonimizate și le prezintă într-o formă ușor de interpretat.

În noua versiune a platformei, au fost îmbunătățite secțiunile de statistici și componenta de analiză (insights), care prezintă sursa atacurilor, totalul atacurilor în funcție de impact și de industrie, din ultimele 30 de zile. De asemenea, a fost adăugată o secțiune în care sunt analizate săptămânal, în mod anonimizat și neinvaziv, cele mai vizitate 100 de website-uri conform SATI (BRAT). Aici utilizatorii pot afla informații cu privire la nivelul actual de securitate al website-urilor și să înțeleagă mai bine riscurile de utilizare ale celorlalte site-uri. Aceste actualizări se bazează pe informații oferite de Pentest-Tools și Dekeneas, ambele startup-uri Orange Fab, și de RO Hacked.

