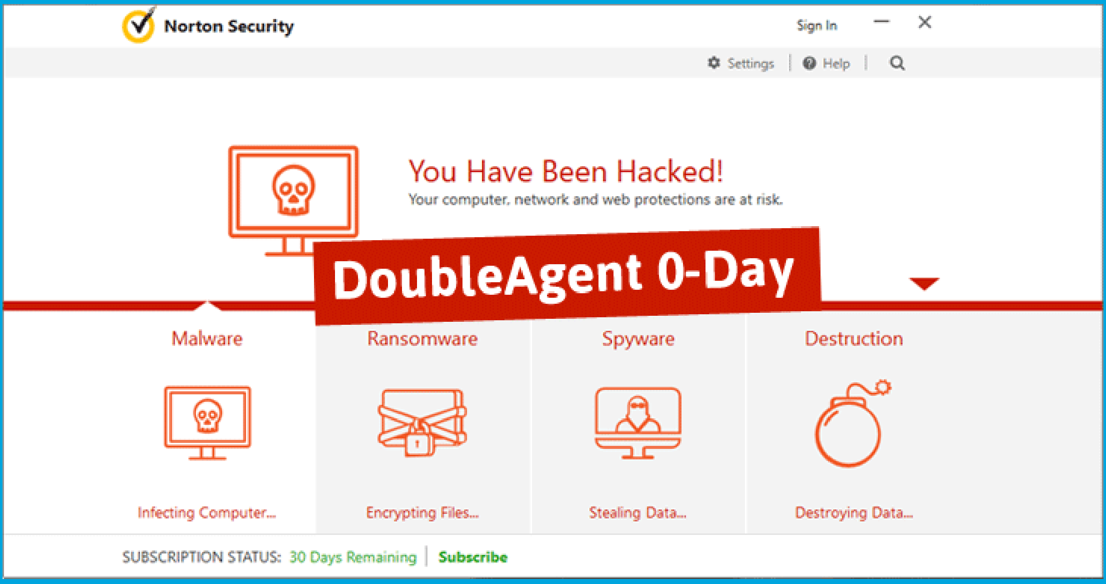
kindred

Security Newsletter

24 March 2017

New 'DoubleAgent' Attack Can Hijack All Windows Versions — Even Your Antivirus!



A team of security researchers from Cybellum, an Israeli zero-day prevention firm, has described a new Windows vulnerability that could allow hackers to take full control of your computer. Dubbed DoubleAgent, the new injecting code technique works on all versions of Microsoft Windows operating systems, starting from Windows XP to the latest release of Windows 10.

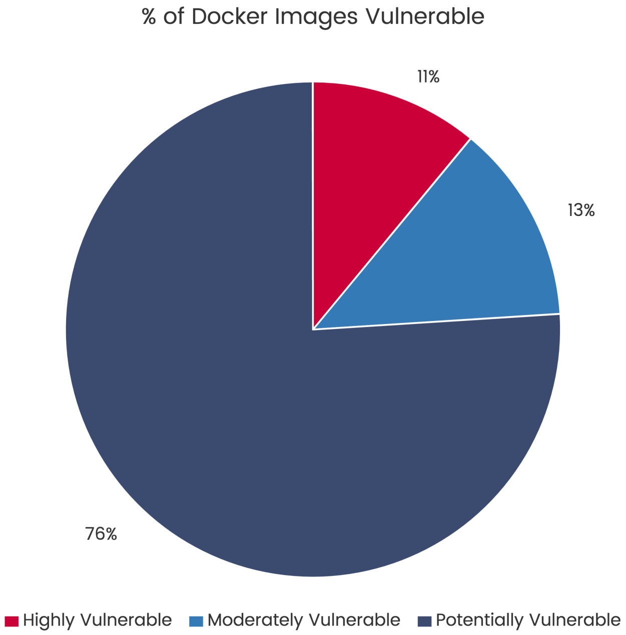
Application Verifier is a runtime verification tool that loads DLLs (dynamic link library) into processes for testing purpose, allowing developers quickly detect and fix programming errors in their applications. The vulnerability resides in how this Application Verifier tool handles DLLs. According to the researchers, as part of the process, DLLs are bound to the target processes in a Windows Registry entry, but attackers can replace the real DLL with a malicious one. It is hard to block because the malicious code can be re-injected into the targeted legitimate process after the system reboots — Thanks to the persistent registry key.

In order to demonstrate the DoubleAgent attack, the team hijacked anti-virus applications -- which is the main defense on systems to prevent any malware from running -- using their technique and turn them into malware. The team was able to corrupt the anti-virus app using the DoubleAgent attack and get the security software to act as disk-encrypting ransomware.

Read More

Initial press release

24% of latest Docker images have significant vulnerabilities



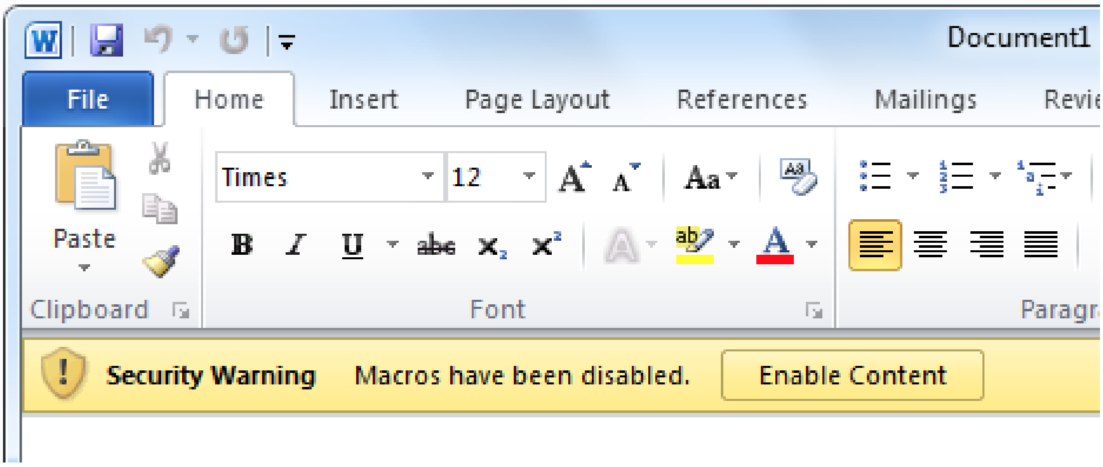
Understanding the vulnerability landscape in the container ecosystem is critical to our mission of securing the world, so we decided to put our technology to work to answer a key question: what is the current state of vulnerabilities in official Docker repositories?

The official Docker repositories consist mostly of images for open source and commercial software, are generally managed by the author or vendor, and contain the most widely used images in the Docker community. Increasingly, they are used as the base for distributed systems replacing some of the functionality of 3rd generation configuration management software.

While the containerization approach offers a lot of benefits, such as enhanced segregation between services, it also makes security patching a lot more challenging. Thankfully, vulnerability scanning of those containers base image is getting easier with open source tools such as Vuls and Clair.

Read More

Word Document Spreads Macro Malware Targeting Both Windows and macOS



Security Warning Macros have been disabled. Enable Content

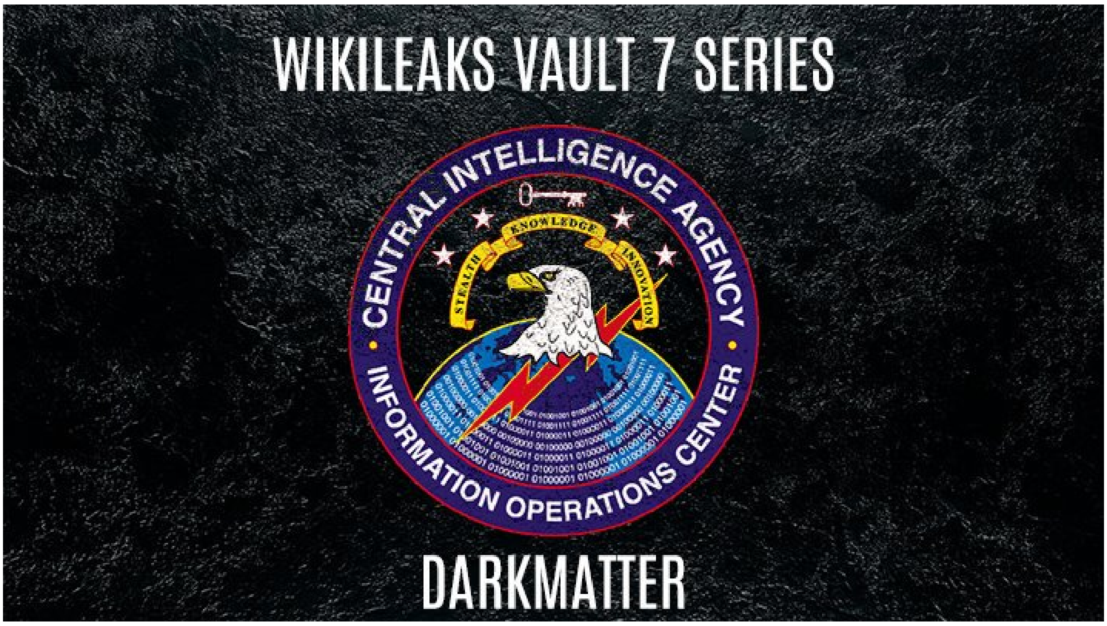
After last month security researchers discovered the first-ever Word document spreading macro malware on macOS, last week, researchers from Fortinet spotted a Word document that contained macro scripts that distributed both Windows and macOS malware at the same time, depending on the OS it managed to infect.

Malicious Office files with attached macro scripts that download malware are usually referred in the infosec industry as "macro malware." On Windows, macro malware has been around since the 90s. Even if Microsoft offered an Office version for Mac OS X (now macOS), weaponized Office files never contained macro scripts that could run on a Mac.

The difference is that at the start of its malicious routine, the macro would check what OS the user was using, and delivered two different versions of the malicious Python code. **MacOS users should take note and be aware of this new attack vector.**

Read More

Wikileaks drops 'Dark Matter', part two of its Vault 7 CIA leaks



Released to the public on March 23, 2017, the second set of documents has been called 'Dark Matter'. Like with part one, it is said to include details of the CIA's global hacking program, and these documents describe hacking methods allegedly used by the agency to access Apple devices and upload data.

In particular, **the documents explain the techniques used by CIA to gain 'persistence' on Apple Mac devices, including Macs and iPhones using, among others, the "Sonic Screwdriver" project.** As explained by the CIA, Sonic Screwdriver was a 2012 "mechanism for executing code on peripheral devices while a Mac laptop or desktop is booting". This would allow an attacker to boot its software from a USB stick, for example, "even when a firmware password is enabled".

Apple has responded to the disclosures from Wikileaks by saying it has completed a preliminary investigation on the new information. “Based on our initial analysis, the alleged iPhone vulnerability affected iPhone 3G only and was fixed in 2009 when iPhone 3GS was released,” the company said in a statement. “Additionally, our preliminary assessment shows the alleged Mac vulnerabilities were previously fixed in all Macs launched after 2013.”

Read More

Dark Matter leak

LastPass bugs could have allowed malicious websites to steal passwords

LastPass patched three separate bugs that affected its Chrome and Firefox browser extensions, which if exploited, would have allowed a third-party to extract passwords from users visiting a malicious website. All bugs were discovered by Tavis Ormandy, a security researcher working for Google's Project Zero. One bug affected the LastPass for Chrome extension, while the other two affected the company's Firefox add-on.

Ormandy put together proof-of-concept code that executes code on a user's machine via this intermediary script and launches an instance of the Windows Calculator. All OS platforms are affected, not just Chrome on Windows. This PoC code can be altered to steal user passwords before they are copied and filled inside username and password fields.

Lastpasss investigation to date has not indicated that any sensitive user data was lost or compromised. All extensions have been patched and are being re-released to users. No master password change is required. No site credential passwords need to be changed.

Any of these vulnerabilities should not keep users from installing a password manager, as wisely pointed out by some well-known security professionals, "your odds of being pwned by a LastPass issue are far lower than if your password is disclosed from one site and reused on another".

Read More

Lastpass report

Google Chrome to Distrust Symantec SSLs for Mis-issuing 30,000 EV Certificates

Google announced its plans to punish Symantec by gradually distrusting its SSL certificates after the company was caught improperly issuing 30,000 Extended Validation (EV) certificates over the past few years.

Extended validation certificates are supposed to provide the highest level of trust and authentication, where before issuing a certificate, Certificate Authority must verify the requesting entity's legal existence and identity.

Symantec has responded and stated that the claim of mis-issuing 30,000 SSL certificates made by Google are "Exaggerated and Misleading". Symantec issues more than 30% of the web's certs, and these are the most popularly relied-upon certs by web-users, constituting 42% of the certs that a Firefox user will encounter in a typical browsing session.

Read More

Pwn2Own hacking contest ends with two virtual machine escapes

Two teams of researchers managed to win the biggest bounties at this year's Pwn2Own hacking contest by escaping from the VMware Workstation virtual machine and executing code on the host operating system.

One of the main goals of hypervisors like VMware Workstation is to create a barrier between the guest operating system that runs inside the virtual machine and the host OS where the hypervisor runs. That's why VM escape exploits are highly prized, more so than browser or OS exploits. **VM escape vulnerabilities could allow malwares to escape scanning sandboxes, or allow an attacker to move from one AWS server instance to another.**

Apple's Safari fell four times, Mozilla Firefox once, but Google Chrome remained unscathed. Researchers also demonstrated two exploits for Adobe Reader and two for Flash Player, both with sandbox escapes. The contest also included many privilege escalation exploits on Windows and macOS.

Read More

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with over 15 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 13 subsidiaries and brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and as an innovation driven company that builds on trust.