kindred

Security Newsletter

30 October 2017

Subscribe to this newsletter

Bad Rabbit ransomware spreading like wildfire, how to stop it

The ransomware, named as Bad Rabbit, is spreading like wildfire and has targeted corporate networks in Russia, Germany, Ukraine, and Turkey mainly. This is a Petya type ransomware that has launched targeted attacks in the past few hours. After successfully compromising the system and encrypting the data, attackers demand 0.05 bitcoin, approx. $285 as ransom to hand over decryption key.

Bad Rabbit is distributed through drive-by download attacks and utilizes fake Adobe Flash players installers to trap victims into installing malware. The victim is required to manually execute the ransomware dropper, which is downloaded from the attacker's infrastructure.

Earlier it was reported that this week's crypto-ransomware outbreak did not use any National Security Agency-developed exploits, neither EternalRomance nor EternalBlue, but a recent report from Cisco's Talos Security Intelligence revealed that the Bad Rabbit ransomware did use EternalRomance exploit. It also utilizes Mimikatz post-exploitation tool to obtain credentials from infected systems.

There is a "Vaccination for Bad Rabbit". Create the following files c:\windows\infpub.dat && c:\windows\cscc.dat – remove ALL PERMISSIONS (inheritance) and you are now vaccinated from the current known samples.

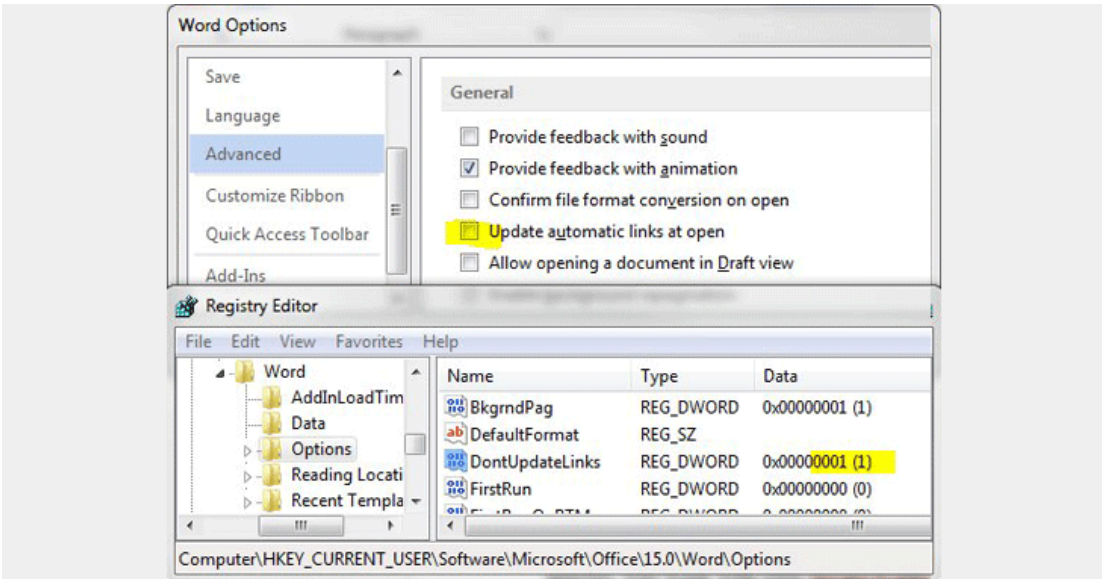
To protect your network, you need to disable WMI service which will not let the malware spread. Moreover, users must remain cautious while clicking on attachments and web links sent by unknown senders via emails and avoid downloading software from third-party platforms.

Read More

Tech details and IoC

Bad Rabbit Uses 'EternalRomance' NSA Exploit

New phishing campaign uses 30-year-old Microsoft mess as bait



A newly discovered unpatched attacking method that exploits a built-in feature of Microsoft Office is currently being used in various widespread malware attack campaigns. The old Microsoft Office feature is called Dynamic Data Exchange (DDE) and allows to perform malicious code execution on the targeted device without requiring Macros enabled or memory corruption.

DDE protocol is one of the several methods that Microsoft uses to allow two running applications to share the same data. The protocol is being used by thousands of apps, including MS Excel, MS Word or Visual Basic. The DDE exploitation technique displays no "security" warnings to victims, except asking them if they want to execute the application specified in the command—although this popup alert could also be eliminated "with proper syntax modification."

Locky ransomware hackers previously relied on macros-based booby-trapped MS Office documents, but now they have updated the Nercus Botnet to deliver malware via the DDE exploit and gain an ability to take screenshots of the desktops of victims.

Since DDE is a Microsoft's legitimate feature, most antivirus solutions do not flag any warning or block MS Office documents with DDE fields. So, you can protect yourself and your organisation from such attacks by disabling the "update automatic links at open" option in the MS Office programs. To do so, Open Word → Select File → Options → Advanced and scroll down to General and then uncheck "Update Automatic links at Open."

Read More

DDE attack works in Outlook too

Security pros' advice to consumers: 'We dunno, try 152 things'

A Google-conducted survey of 231 infosec pros worldwide has reaffirmed the industry's faith in strong passwords, and achieved consensus about nothing else.

It's almost unfair to make fun of the study's title, as the document also includes the note, "ED: Please provide section title". What's clear is that infosec types can't agree, on an industry-wide basis. By asking 231 security pros for their top three pieces of advice, the suffering authors of the study (Robert Reeder, Iulia Ion, and Sunny Consolvo) ended up with a list 152 items long. As the paper dryly notes, "future work is needed to distill the 152 pieces of advice and communicate to users the most important ones".

"it's perhaps unsurprising that users don't follow all the advice on offer—there's a lot of it, it spans diverse areas, and it's not clear where to start. Users are probably not receiving a consistent message on what's most important and exactly what to do in each area".

Read More

152 Simple Steps to Stay Safe Online

DUHK Crypto Attack Recovers Encryption Keys, Exposes VPN Connections, etc

After last week we had the KRACK and ROCA cryptographic attacks, this week has gotten off to a similarly "great" start with the publication of a new crypto attack known as DUHK (Don't Use Hard-coded Keys).

The issue at the heart of the DUHK attack is a combination of the usage of the ANSI X9.31 Random Number Generator (RNG) and when hardware vendors use a hardcoded "seed key" for this algorithm. When those two conditions are met, attackers can decrypt encrypted communications carried out through that device. This includes communications passing over VPN connections or encrypted web sessions that carry out login credentials, payment information, Intranet information, private enterprise data, and more.

Researchers reveal they were able to recover encrypted traffic from Fortinet FortiGate devices used by companies across the world as firewalls or to create private VPN networks. They reversed engineered FortiGate firmware images and found the hard-coded seed key. They then observed traffic coming from the affected device and using the seed key, they brute-forced encrypted data to guess the rest of the encryption parameters. This, in turn, allowed them to determine the main encryption key. Fortinet FortiGate devices using FortiOS 4.3.0 to FortiOS 4.3.18 are vulnerable.

The attack is not trivial, but researchers say it's practical as an attacker using a modern computer can recover the encryption key in around four minutes per connection. There is no user interaction needed to carry out a DUHK attack, as all the threat actor needs is a position to observe traffic coming from a vulnerable device. Because this is a passive network attack, victims cannot detect when someone uses a DUHK attack against them. This is because ANSI X9.31 is very widespread. Up until January 2016, the algorithm was on the list of US government (FIPS) approved RNG algorithms.

The research team also warns that other hardware and software products may also be affected by DUHK attacks.

Read More

"Official" page

Reaper botnet could be worse than Mirai

A little over a month ago, a sizable botnet of infected Internet of Things devices began appearing on the radar of security researchers. Just weeks later, it could become one of the largest botnets recorded in recent years.

The botnet, dubbed "Reaper" by researchers at Netlab 360, is was said to have ensnared almost two million internet-connected webcams, security cameras, and digital video recorders (DVRs), putting its growth at a far faster pace than Mirai. But the Reaper IoT botnet is nowhere near as threatening as previously suggested, according to new research. Boffins at Arbor Networks, however, estimate that the actual size of the Reaper botnet tends to fluctuate between 10,000-20,000 bots, but warn that this number could change at any time.

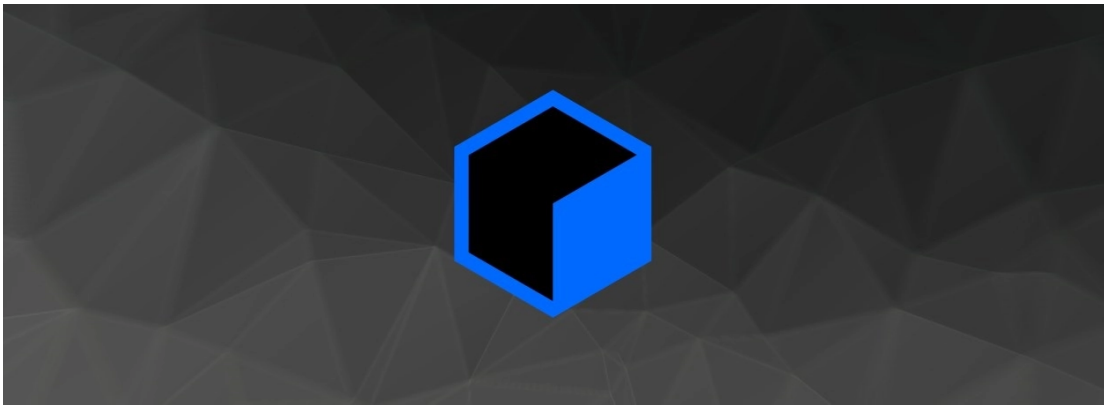
Mirai aggressively ran each device against a list of known usernames and passwords, but Reaper is "not very aggressive," said Netlab. By targeting a known vulnerability, the botnet can swiftly take control of a device without raising any alarms. Netlab said at the time of publishing their research that the botnet was infecting nine known vulnerabilities in D-Link, Netgear, and AVTech products, as well as other device makers.

Read More

Initial article from Netlab

Reaper IoT botnet ain't so scary

Hacker Takes Over Coinhive DNS Server After Company Reuses Old Password



Monero miner maker Coin Hive was hacked so that websites using its code inadvertently redirected their generated cryptocurrency to miscreants – after the outfit forgot to change an old password.

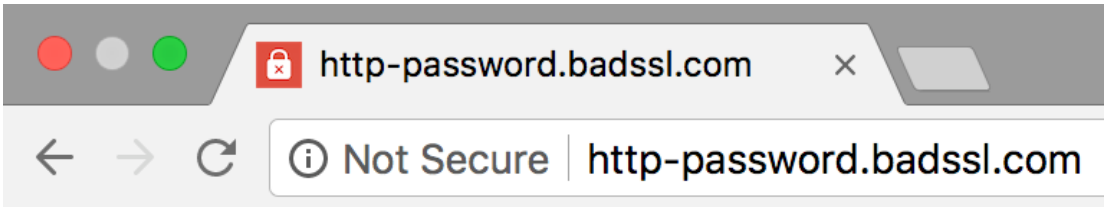
"The DNS records for coinhive.com have been manipulated to redirect requests for the coinhive.min.js to a third party server," it said in a blog post. "This third party server hosted a modified version of the JavaScript file with a hardcoded site key. This essentially let the attacker 'steal' hashes from our users." Coin Hive said it regularly changes its passwords and uses two-factor authentication on its main accounts, but its Cloudflare account was overlooked. It thinks the password was the same one its team used on Kickstarter, which was hacked in February 2014 and the Cloudflare pass phrase hadn't been changed since.

The cockup highlights the dangers of reusing pass phrases and not setting up two-factor authentication for everything. There are plenty of databases out there with searchable passwords, email addresses and usernames, collected from various hacked websites and services. So if you're reusing credentials on multiple systems, you'll eventually be caught out when one of those systems is compromised and the login details for, essentially, all your accounts are leaked.

Read More

Even More

Performing and Preventing SSL Stripping: A Plain-English Primer



Over the past few days we learnt about a new attack that posed a serious weakness in the encryption protocol used to secure all modern Wi-Fi networks. The KRACK Attack effectively allows interception of traffic on wireless networks secured by the WPA2 protocol. Whilst it is possible to backward patch implementations to mitigate this vulnerability, security updates are rarely installed universally.

It is beyond doubt that it is simply not secure to blindly trust the medium that connects your users to the internet. HTTPS was created to allow HTTP traffic to be transmitted in encrypted form, however the authors of the KRACK Attack presented a video demonstration of how the encryption could be completely stripped away on a popular dating site (despite the website supporting HTTPS).

This blog post presents a plain-english primer on how HTTPS protection can be stripped and mechanisms for mitigating this.

Read More

Cutting room floor

- Microsoft's new open source tool can scan your website for security and performance headaches
- Surveying 17 Anti-Virus Firms on Their Security Practices
- Quick web pentest of Sarahah
- Introducing Miscreant: a multi-language misuse resistant encryption library
- Windows 10's "Controlled Folder Access" Anti-Ransomware Feature Is Now Live
- Now You Can Use Amazon ElastiCache for Redis with In-Transit and At-Rest Encryption to Help Protect Sensitive Information
- Time To Update Your Vacuum Cleaner -- Hack Turns LG Robot Hoover Into A Spy
- Target="_blank" - the most underestimated vulnerability ever
- EU law bods closer to baking new 'cookie law' after battle
- Google Play Protect is last at detecting known malware on Android
- Lab for Java Deserialization Vulnerabilities
- AI Bot That Mimics the Human Eye Breaks reCAPTCHAs With 66.6% Accuracy
- Android takes aim at ISP surveillance with DNS privacy

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.

You can access the previous newsletters at https://news.infosecgur.us