SWITCHcert report on current trends in the field of IT security and privacy

July/August 2017

SWITCH

I. Family business: Petya and its derivatives sweep over half the world as a new wave of ransomware

Less than two months after the global attack of the blackmail Trojan WannaCry and its derivatives, a second wave of ransomware is sweeping half of the world. Security researchers initially assumed that they were dealing with a new descendant of Petya, the cryptolocker first launched in 2016. Its four varieties, which could be distinguished by the colour of the skull appearing on the screens of affected computers, and the related ransomware derivatives Goldeneye and Mischa, infected several computers via fake PDF files contained in emails, primarily in 2016. They encrypted the hard drive indexes and/or files of their targets (a detailed summary can be found on Wikipedia, among other sites). On 5 July, the hacker group Janus Cybercrime, then already suspected of developing the Trojan, published a master key that was confirmed as genuine. The key restored access to files and hard drives affected by Petya, Mischa or Goldeneye.

But soon after the outbreak of the alleged new Petya derivative in late June, several security researchers pointed out that NotPetya, as it has been dubbed since, constituted a whole new level of virus that has little in common with the Petya family of ransomware. Rather than money, NotPetya apparently aims for the complete destruction of all data on the compromised devices: it is a so-called «wiper» rather than a blackmail Trojan. An in-depth analysis of the damage has shown that the authors of this ransomware are incapable of restoring any data even if a ransom had been paid. Most experts therefore suspect that political motives rather than greed are behind NotPetya. In addition, NotPetya is not disseminated via phishing emails or email attachments; in Ukraine, it was hidden in updates for a software suite used by many taxpayers. Some researchers claim that the NotPetya authors may simply have done sloppy work, however.

Read more:

https://en.wikipedia.org/wiki/Petya
https://www.heise.de/security/meldung/Rueckkehr-von-Petya-Kryptotrojaner-legt-weltweit-Firmen-und-Behoerden-lahm-3757047.html
https://www.theregister.co.uk/2017/06/28/petya_notpetya_ransomware
https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how
https://www.heise.de/security/meldung/Alles-was-wir-bisher-ueber-den-Petya-NotPetya-Ausbruch-wissen-3757607.html?artikelseite=3
https://www.heise.de/security/meldung/Master-Schluessel-der-Erpressungstrojaner-GoldenEye-Mischa-und-Petya-veroeffentlicht-3767637.html
https://www.heise.de/security/meldung/Petya-NotPetya-Kein-Erpressungstrojaner-sondern-ein-Wiper-3759293.html
https://www.netzwelt.de/news/160887-keylogger-hp-notebook-hersteller-veroeffentlicht-statement.html

II. Pay a ransom for your privacy: new «extortionware» exposes its victims

In cyberspace, almost nothing is impossible. Just as we have got our heads around the blackmail Trojans – WannaCry, Petya and the like – that request a ransom from the users of affected devices to release their data, a new type of malicious software is on the rise. The authors of «LeakerLockers» threaten to send all data found on the compromised Android smartphones and tablets to all stored contacts, should the owners of the devices fail to pay the requested ransom of USD 50 in Bitcoin. This type of ransomware with its «innovative business model» claims to be able to expose browser histories, photographs, emails and Facebook messages. But the McAfee security experts who first discovered the software have proven that these claims are only partially founded, as described in the fact sheet linked below. By now, Google has removed both apps that hosted the malicious software (Booster & Cleaner Pro and Wallpapers Blur HD) from its Play Store.

Nonetheless, many security experts are concerned about these developments. They fear that the «LeakerLockers» may just be the modest beginning of a larger wave of «extortionware», considering the enormous potential of the concept.

Read more:

https://futurezone.at/digital-life/ransomware-droht-browserverlauf-an-alle-kontakte-zu-senden/274.616.209
https://securingtomorrow.mcafee.com/mcafee-labs/leakerlocker-mobile-ransomware-acts-without-encryption
https://www.infosecurity-magazine.com/news/leakerlocker-extortionware
https://www.hackread.com/leakerlocker-android-ransomware-pay-or-data-leak
http://www.independent.co.uk/life-style/gadgets-and-tech/news/leakerlocker-malware-leaked-photos-ransom-pictures-internet-history-messages-privacy-security-send-a7838836.html

III. Positive use of metadata – Cisco can detect malware activity even in encrypted network traffic

In our last SWITCHcert report, we explained how metadata can be utilised to de-anonymise internet users in order to use or sell their profiles for advertising purposes. Research by three Cisco employees, Blake Anderson, Subharthi Paul and David McGrew, has now shown that metadata can be used more positively, too. Their work highlights a way of detecting malware even when it is hidden behind encryption protocols such as TLS (the successor of the well-known SSL protocol used for safe data transfers on the internet).

Anderson and his co-authors have successfully trained a machine learning system to distinguish the type of network traffic that installs malware from legitimate data traffic – with a reliability of more than 99 percent and without interrupting the TLS encryption. Instead, the system focusses primarily on metadata, which also exists in encrypted traffic. This includes NetFlow data (ports, bytes in/out, duration, etc.), typical packet lengths (Sequence of Packet Lengths and Times, SPLT), the distribution of bytes and, above all, unencrypted TLS header files.

Even though the researchers» paper (see first source link below) itself describes a way of circumventing this detection mechanism, it highlights that there may well be alternative approaches to breaking of encryption protocols, both in terms of data protection and security, which deserve to be more closely studied.

Read more:

https://arxiv.org/pdf/1607.01639.pdf
https://www.heise.de/security/artikel/Cisco-analysiert-verschluesselten-Traffic-um-Malware-zu-erkennen-3753229.html
http://cloud-practice.de/hintergrund-cisco-analysiert-verschlusselten-traffic-um-malware-zu-erkennen

IV. Successful strike against the darknet drug and weapons trade – security services bust AlphaBay and Hansa

Without breaking encryption protocols, however, one of the most spectacular investigative successes by international security authorities would have been impossible: in July, the FBI, Europol and the public prosecutor's office of Frankfurt am Main reported that they had shut down AlphaBay and Hansa, two trading platforms for hard drugs, weapons, counterfeit currency, fake identification documents, malware and hacked credit card and online account data, and arrested their operators. The effort was closely coordinated with Canadian, French, Thai, Lithuanian and other international investigators. With more than 40,000 traders, 200,000 customers and a daily turnover in the high six figures, AlphaBay was considered the main trading centre for illegal goods and services on the darknet.

As positive as the news of the AlphaBay and Hansa bust may be, however, a certain painful ambivalence remains: the darknet is not exclusively a safe haven for criminals, terrorists, cyber-racketeers and other scoundrels. It also often functions as the only refuge for opposition groups, dissidents, journalists and whistle-blowers in dictatorships and rogue states. During the online debate about the risk society held by the Federal Agency for Civic Education, Christian Mihr, CEO of Reporters Without Borders called spaces of digital anonymity an essential component of democratic societies. Sites from Facebook to netzpolitik.org mirror their content on .onion pages in order to grant people living under repressive regimes anonymous access to the information available there. During the same debate, the Director of the Centre of European and International Criminal Law at the University of Osnabrück demanded the decryption of the darknet on account of its protective function for severe crimes and criminals. And it seems that security and intelligence services are becoming increasingly proficient at that approach. This is good news for the fight against those who abuse the darknet for criminal purposes, but bad news for its «good» users, who are in need of protection and at risk of losing their last refuge.

Read more:

https://www.nzz.ch/digital/aktuelle-themen/erfolg-im-bereich-cyber-crime-geglueckte-ermittlung-gegen-darknet-struktur-ld.1307107
http://www.sueddeutsche.de/digital/alpha-bay-ermittler-heben-groessten-illegalen-darknet-marktplatz-aus-1.3597381
http://www.chip.de/news/AlphaBay-Portal-Betreiber-haeufte-im-Darknet-gigantisches-Vermoegen-an_119390997.html
https://www.bpb.de/dialog/netzdebatte/239003/das-darknet-als-geschuetzter-raum-gegen-ueberwachung-und-selbstzensur
https://www.bpb.de/dialog/netzdebatte/242957/das-darknet-ein-paradies-fuer-kriminelle
https://motherboard.vice.com/de/article/d7yakj/bundesregierung-versucht-das-darknet-zu-erklaeren-und-zeigt-wie-kompliziert-das-alles-eigentlich-ist

This SWITCH-CERT security report was written by Dieter Brecheis and Michael Fuchs.

The security report does not represent the views of SWITCH; it is a summary of various reports published in the media. SWITCH does not assume any liability for the content or opinions presented in the security report nor for the correctness thereof.