A brief study of malicious virus: Ransomware

Ashok P[1] Akhila G[2] Anitha J[3]

Assistant Professor[1]
UG Scholar [2,3]
Department of Computer Science and Engineering[1, 2, 3]
Sri Sai Ram Institute of Technology, Tamilnadu, India

ABSTRACT -Ransomware is a type of malicious software that blocks access to the victim's data or threatens to publish or delete it until a ransom is paid. Ransomware attacks are typically carried out using a Trojan that is disguised as a legitimate file that the user is tricked into downloading or opening when it arrives as an e-mail attachment. The concept of file encrypting ransomware was invented and implemented by Yung and Yong at Columbia university and was presented at the 1996 IEEE Security and privacy conference called crypto viral extortion, in which it encrypts the victim's files, making them inaccessible. Android was taken the world of mobile computing to the whole different level and made possible persuasive interaction between user and mobile service. Although it is a Linux based OS, most hackers and cyber criminals have found a way to manipulate it to their best interests. Of late more than 300 malware categories have been discovered since the advent of android and most lethal being Ransomware and Trojan. This paper seeks to highlight the computer security threats witnessed from 2016-17, enhancement fighting techniques employed in computer and mobile system.

KEYWORDS: Ransomware, Trojan, malicious, crypto viral extortion

I. INTRODUCTION

Ransomware is a type of malware which tries to extort users of the infected systems. It will then ask for ransom from the owners to make their own devices accessible. In June 2013, first ransomware called "Cryptolocker" was discovered. It was targeted to android devices. Hidden under the name of an antivirus called "Android Defender". Similarly, the famous ransomware that was Trojan called "Obad". It can rack up the phone bill by sending premium SMS to the favour of Trojan owner. In a properly implemented cryptoviral extortion attack, recovering the files without the decryption key is an intractable problem- and difficult to trace digital currencies used for the ransoms, making tracing and prosecuting the perpetrators difficult. Starting from around 2012 the use of ransomware scams has grown internationally. In June 2013, security software vendor McAfee released data showing that it had collected more than double the number of samples of ransomware that quarter than it had in the same quarter of the previous year. Payments is virtually always the goal, and the victim is coerced into paying for the ransomware to be removed which may or may not actually occur either by supplying a program that can decrypt the files, or by sending an unlock code that undoes the payload's changed. A key element in making ransomware work for the attacker is a convenient payment system that is hard.

II. HISTORY

Encrypting Ransomware

The first malware extortion Attack, the "AIDS Trojan" written by Joseph Popp in 1989, had a design failure so severe it was not necessary to pay the extortionist at all. Its payload hid the files on the hard drive and encrypted only their names, and displayed a message claiming that the user's licenses to use a certain piece of software have expired. The user was asked to pay US $189 to "PC Cyborg Corporation" in order obtain repair tool even though the decryption key could be extracted from the code of the Trojan. The idea of abusing anonymous cash systems to safely collect ransomware from women kidnapping was introduced in 1992. This money collection method is a key feature of ransomware. The notion of using public key cryptography for data kidnapping attacks was introduced in 1996 by Adam L. Yung and Yong. Encrypting ransomware returned to prominence in late 2013 with the propagation of cryptolocker to collect ransom money.

Non-Encrypting Ransomware:

In 2010, Russian authorities Arrested nine individuals connected to a ransomware Trojan knows as WinLock which do not use encryption. Instead, WinLock trivially restricted access to the system by displaying pornographic images, and asked users

to send a premium rate SMS(costing around US $10) to receive a code that could be used to unlock their machines. In 2011, an online activation option was offered but was unavailable requiring the users to call one of six international numbers to input a six digit code. While the malware claimed that this call would be free, it was routed through a rogue operator in a country with high international phone rates, who place the call on hold, causing the user to incur large international long distance charges.

2.1 Leakware

The converse of ransomware is a cryptovirology attack that threatens to publish stolen information from the victim's computer system rather than deny the victim access to it. "The attack differs from the extortion attack in the following way. In the extortion attack, the victim denied access to its own valuable information and has to pay to get it back, where in the attack that is presented here the victim retains access to the information but its disclosure is at the discretion of the computer virus.

2.2 Mobile ransomware

With the increased popularity of ransomware on PC platforms, ransomware targeting mobile operating systems has also proliferated. Mobile ransomware targets the Android platform, as it allows applications to be installed from third party sources. The payload typically distributed as an APK files installed by an unsuspecting user; it may attempt to display a blocking message over top of all other applications.

III. TYPES OF RANSOMWARE

Crypto Ransomware

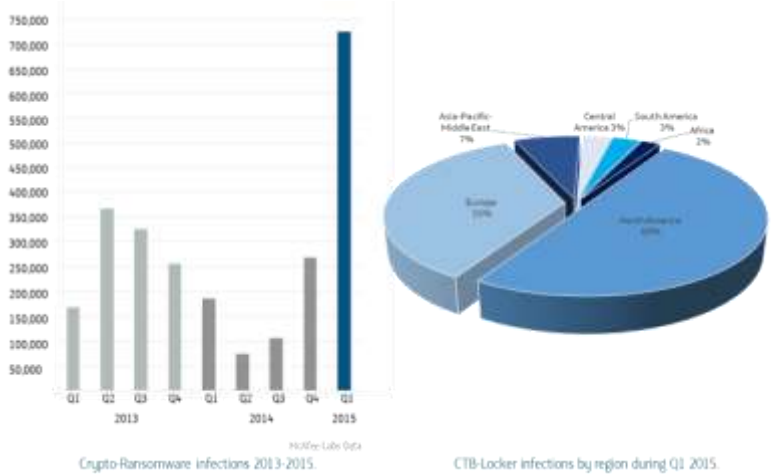
Crypto ransomware is as simple as weaponizing strong encryption against victim to deny them access to those files. Once the ransomware infiltrates the victim's device, the malware silently identifies and encrypts valuable files. Only after successfully accessing to target files as been restricted does the ransomware ask the user for a fee to access their files. Without the decryption key held by the attackers, or in some cases, a vendor decryption solution, the user loses access to the encrypted files. Crypto ransomware often includes a time limit. Some variants of crypto ransomware even provide users with a site to purchase Bitcoins and articles explaining a currency.

3.1 Locker Ransomware

This is also known as computer locker. This ransomware doesn't encrypt the files of the victim but instead, it denies the access to the device. This locks the device's user interface and then demands the victim for the ransom. This ransomware will leave the victim with very few capabilities such as allowing the victim just to communicate with the attacker and to pay the ransom.

3.2 Wannacrypt

The WannaCry ransomware attack spread through the internet, using an exploit vector that Microsoft had issued a "Critical" patch. The ransomware infected over 75000 users in over 99 countries, using 20 different languages to demand money from users using Bitcoin crypto currency. Wannacrypt demanded $300 per computer. The attackers gave their victims a 7-day deadline from the day their computers got infected, after
which the encrypted files would be deleted.



Crypto-Ransomware infections 2013-2015. CTB-Locker infections by region during Q1 2015.

Fig1. Wannacrypt

3.4. **Torrent Locker**

Torrent Locker is spread principally through spam emails. In addition to the standard procedures of encrypting files of multiple types and demanding a ransom in Bitcoin, this ransomware also harvests email address found on the machine and uses these to send further spam emails to the victim's contacts in an attempt to propagate further. TorrentLocker attempts to delete Windows volume shadow copies to make it less likely that users can recover their files without paying the ransom. This is normally set at about $ 500 if paid within three days, payable in Bitcoin to an address which differs for each victim

3.5 Petya:

In June 2017, another type of complex ransomware has infected computers worldwide. It goes by the name of 'Petya', and it caused companies like DLA Piper and Maersk to freeze up their systems. The only way for these companies to have unlock their systems, is, of course by paying a hefty ransomware. The interesting thing about the Petya virus is that the authors of Petya demanded the large ransom (100-bitcoin) only after many companies infected already resumed their operations. Though it looks like some victims had decided to pay a smaller ransom, Petya's financial success didn't amount too much. Petya infiltrated networks through systems that used Microsoft Windows and although it seems that Petya's main goal was to disrupt Ukrainian infrastructure rather than just make money.

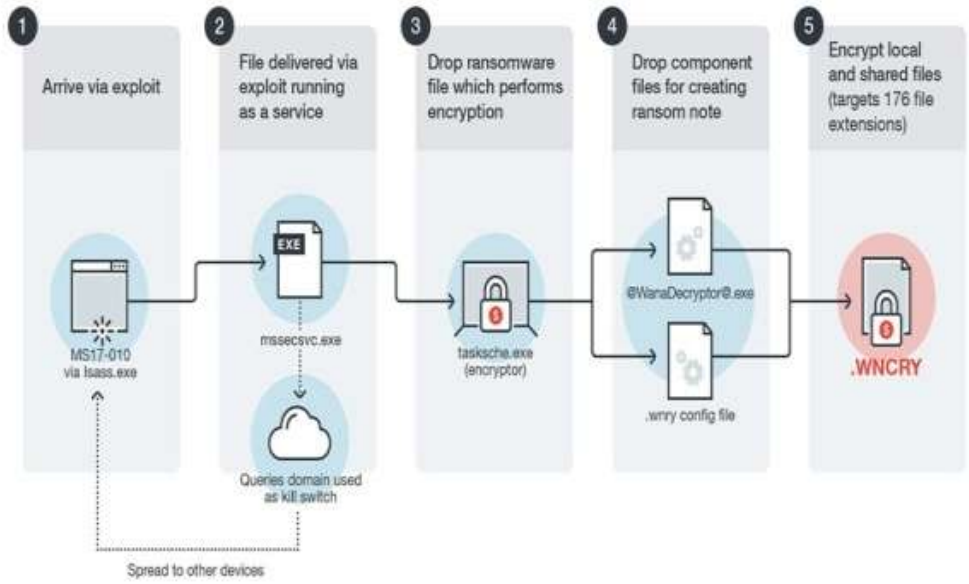
PROPAGATION OF RANSOMWARE

Ransomware is typically spread and delivered through social engineering and user interaction, opening malicious email attachments, clicking on a malicious link within an email or on a social networking site. It can be disguised as fake PDF files in email attachments which appear to be legitimate correspondence from reputable companies such as banks and other financial institutions. Attackers will use email addresses and subjects that will entice a user to read and open the file. Some attackers will use Shortened malicious URLs to mask a malicious destination and malicious script downloader. Still another technique uses spam emails and social engineering to infect a system by enticing users to open an infected word document with embedded macro viruses and convince them to manually enable macros that allow the malicious code to run. Crypto malware can also be delivered via malvertising attacks, exploit kits and drive-by downloads when visiting compromised websites. An Exploit Kit is a malicious tool with pre-written code used by cyber criminals to exploit vulnerabilities in outdated or insecure software applications and then execute malicious code. Currently the Angler, Magnitude, Neutrino and Nuclear exploit kits are the most popular.

RaaS (Ransomware as a Service) is a ransomware hosted on the TOR network that allows "affiliated" to generate a ransomware and distribute it any way they want. The RaaS developer will collect and validate payments, issue decrypters and send ransom payments to the affiliate, keeping 20% of the collected ransoms. Another scenario has involved attackers installing and spreading ransomware by targeted Remote Desktop or Terminal Services Attacks, especially on servers. The attacker brute forces weak passwords on computers running Remote Desktop or Terminal Services. Once the attacker gains access to a target computer, they download and install a package that generates the encryption keys, encrypts the data files, and then uploads various files back to the hacker via the terminal services client. Kaspersky has reported brute force attacks against RDP servers are on the rise.

4.1 About Encryption

Crypto malware encrypts any data file that the victim has access to since it generally runs in the context of the user that invokes the executable and does not need administrative rights. It typically will scan and encrypt whatever data files it finds on computers connected in the same network with a drive letter including removable drives, network shares and even DropBox mappings. If there is a drive letter on your computer it will be scanned for data files and encrypt them. Some malware will scan all of the drive letters that match certain file extensions and when it finds a match, it encrypts them. Some of the more popular ransomware use RSA encryption, AES encryption or a combination such as ECC (Elliptic Curve Cryptography) to encrypt data. RSA uses asymmetric key encryption algorithm which utilizes a key pair system, a public and a private key. Encryption with the public key can only be decrypted by the private key generated and stored on the command- and-control server used by the malware creators. Since the private key cannot be calculated from the public key, these properties make decryption impossible.
AES uses symmetric key algorithm encryption and shares the same (single, secret) cryptographic key for both encryption and decryption. AES has a fixed size of 128-bits and permits the use of 128,192 or 256-bit keys. Breaking a symmetric 256-bit key by brute force requires several thousand times more computational power than a 128-bit key.



. Fig2. Attack of ransomware

WAYS FOR REMOVING RANSOMWARE WHEN OCCURS IN WINDOWS

If you have the simplest kind of ransomware, such as a fake antivirus program or a bogus clean-up tool, you can usually remove it by the following the steps in my previous malware removal guide. This procedure includes entering Window's Safe Mode and running an on-demand virus scanner such as Malware bytes.

If the ransomware prevents you from entering Windows or running programs, as lock-screen viruses typically do, you can try to use System Restore to roll windows back in time. Doing so doesn't affect personal files, but it does not return system files and programs to the state they were in at a certain time. The system restore feature must be enabled beforehand; window enables it by default.

5.1 Windows 7

1. Shut down your PC and locate the F8 key on your PC's keyboard.
2. Turn the PC on, and as soon as you see anything on the screen, press the F8 key repeatedly. This action should bring up the Advanced Boot Options menu.
3. Select Repair your computer and press enter.
4. You'll likely have to log on as a user. Select your windows account name and enter your password.
5. Once logged on, click system restore.

5.2 Windows 8, 8.1, or 10:

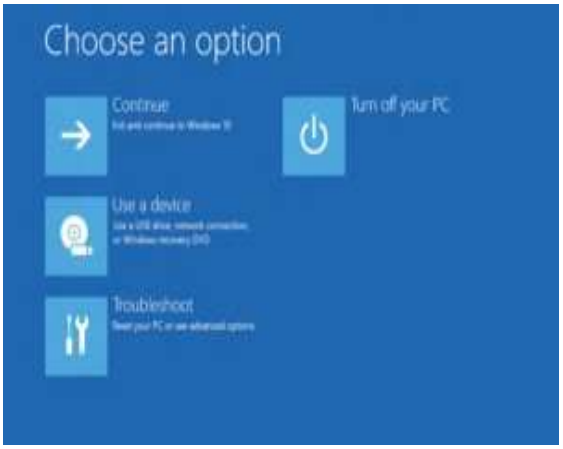


Fig 3.Rebooting PC

You can recover by holding shift when rebooting from the Windows login screen.

1. If your PC boots to the Windows login screen hold the Shift key, click the power icon, and select Restart.
2. It should reboot to the recovery screen.
3. Select Troubleshoot>Advanced Options>System Restore.

With that out of the way, it's time to repair the damage. If you're lucky, your PC was infected by malware that didn't encrypt your data. If it appears you're missing stuff through, the malware may have merely hid your icons, shortcuts and files. It usually does this by making the files "hidden".

6. PREVENTION ADVICE

Back-up! Back-up!:

Have a recovery system in place so a ransomware infection can't destroy your personal data forever. It's best to create two back-up copies: one to be stored in the cloud (remember to use a service that makes an automatic backup of your files) and one to store physically (portable hard drive, thumb drive, extra laptop, etc). Disconnect these from your computer when you are done. Your back up copies will also come in handy should you accidentally delete a critical file or experience a hard drive failure.

2. Use robust antivirus software:

Use robust antivirus software to protect your system from ransomware. Do not switch off the 'heuristic functions' as these help the solution to catch samples of ransomware that have not yet been formally detected.

3. Keep all the software on your computer up to date:

When your operating system or applications release a new version, install it. And if the software offers the option of automatic updating, take it.

4. **Trust no one. Literally**:

Any account can be compromised and malicious links can be sent from the accounts of friends on social media, colleagues or an online gaming partner. Never open attachments in emails from someone you don't know. Cybercriminals often distribute fake email messages that look very much like email notifications from an online store, a bank, the police, a court or a tax collection agency, luring recipients into clicking on a malicious link and releasing the malware into their system.

5. Enable the 'Show file extensions' option in the Windows settings on your computer:

This will make it easier to spot potentially malicious files. Stay away from file extensions like .exe ', '.vbs, '.scr'. Scammers can use several extensions to disguise a malicious file as a video, photo, or document (like hot-chics.avi.exe or doc.scr).

6. If you discover or unknown process on your machine, disconnect it immediately from the internet or other network connections (such as home Wi-Fi)-this will prevent the infection from spreading.

I. WILL THE FUTURE BE SAFE FROM RANSOMWARE?

While the threat from WannaCry has now subsided, the outbreak itself has been a real wake-up call to companies across the globe. It's brought the danger of ransomware into clear focus, and really reiterated the importance of making sure you're no vulnerable to future attacks.

There is a blog recently focussing on email security and some general tips on protecting yourself from scammers which is a valuable read. However, when it comes to malware, and especially ransomware, there are three top tips to minimise the chances of your company being the next victim.

1. Educate your staff on cyber security:

While WannaCry was a little different in that it was a worm, ransomware is often delivered as a loaded hyperlink that is accidently opened through an email, webpage ad or even through social media. Make sure your employees understand what they should and shouldn't be opening or clicking on.

2. Always apply the latest patches:

Those annoying messages you get telling you an update is available? Well, don't ignore them! It's the first line of defence against infection, and your patches should always be up to date. And it's not just Windows; malicious software can spread through other types of software such as Abode and Java, so always install any updates that pop up. Also make sure you're running a supported version of your software. WannaCry targeted versions of Windows such as

XP and 2003 that Microsoft don't even offer updates for any more. Upgrading your systems may seem like an expense you can't justify, but it could cost you even more down the line.

3. **Get the right anti-virus protection**:

Ransomware and malware in general is getting more and more sophisticated, so many of the more traditional anti-viral software may no longer be up to the job. This software traditionally relies on static, signature-based methods to detect ransomware, but just can't keep up with the continuous modifications. Increasingly, the future is in behaviour-based detection mechanisms, which can scrutinise what processes are doing and identify if they are malicious before quarantining and removing them. So talk to your IT team or supplier to ensure your company's systems have the protection they need.

Of course, as a last line of defence you should make sure all your data is regularly backed up. Preferably in a remote, unconnected backup or storage facility so if the worst should happen you can recover your files. But as with most things in life, prevention is very definitely better than cure.

II. PERFORMANCE EVALUATION

Fig 4.countdown starts

From the survey it is clear that Saudi Arabia is ranked 20th and the UAR is ranked 26th globally for ransomware attacks. Saudi Arabia represents 0.7 percent and the UAE about 0.5 percent of all global detections. Couple of highlights in 2016 was that email is becoming, and will become, the most used weapon of choice for attackers. Ransomware attacks have grown 36 percent globally and the preferred source for ransomware is still email while cloud has become the second frontier for attacks.

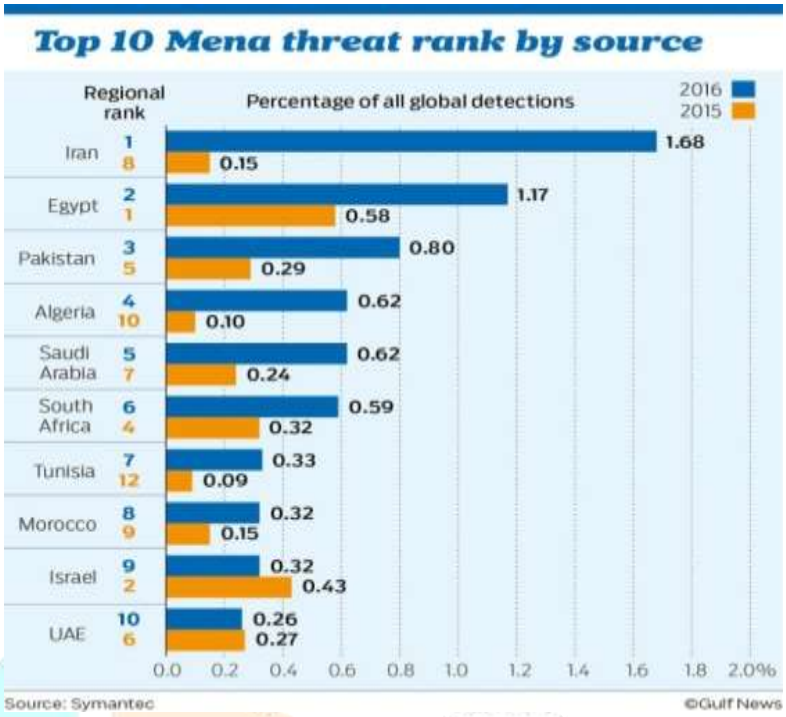


Fig 5.barchart ransomware attack

As s loose global network of cyber security experts fought the ransomware hackers, Chinese state media said 29,372 institutions there had been infected along with hundreds of thousands of devices.

The Japan Computer Response Team Coordination Centre, a non-profit providing support for computer attacks, said 2000 computers at 600 locations in Japan were affected so far. Government agencies said they were unaffected. Companies like Hitachi and Nissan Motor Co. Reported problems they said has not seriously affected their business operations. In China, universities and other educational institutions were among the hardest hit, about 15 percent of the internet protocol addresses attacked, according to the official Xinhua News Agency. That may be because schools tend to have old computers and be slow about updates of operating systems and security. Railway stations, mail delivery, gas stations, hospitals, office buildings, shopping malls and government services also were affected.

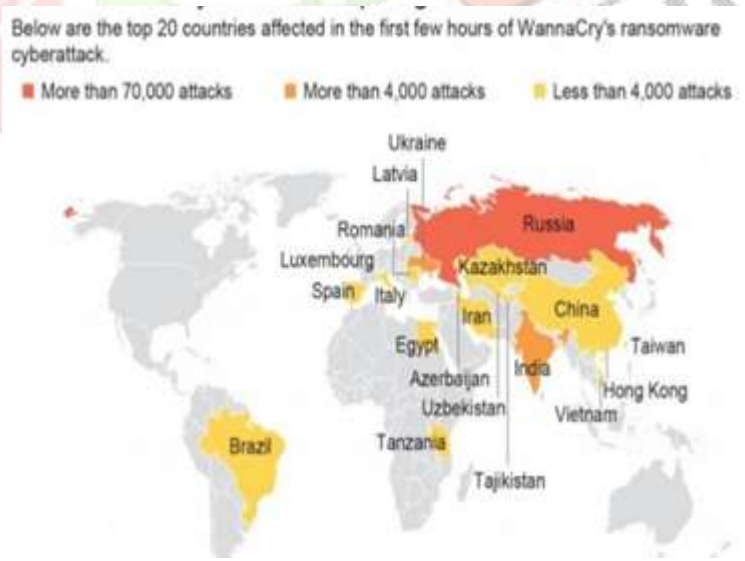


Fig 6. Affected **place**

CONCLUSION

Ransomware attacks, has proved that their impact can be devastating to small business owners and organisation. Ransomware is not only threats to small business and organisation it has an impact on people as well. In its public service request

report from the FBI, they urge anyone who's suffered a ransomware infection to never pay ransom because it helps criminals refine their attacks and share even more victims. Paying a ransom does not guarantee the victim will regain access to their data? In fact, some individuals or organizations are never provided with decryption keys after paying a ransom. The recommendations that would help small business owners and organizations prevent and defend attacks from ransomware are by using Trend Micro Security 10, VIPRE Internet Security Pro Small Office and Kaspersky Internet Security.

REFERENCE

[1]https://heimdalsecurity.com/blog/what-is-ransomware-protection
[2] https://us.norton.com/internetsecurity-malware-7-tips-to-prevent-ransomware.html
[3]https://www.barkly.com/ransomware-protection-and-prevention
[4]https://www.welivesecurity.com/.../11-things-you-can-do-to-protect-against-ransomware
[5] https://combofix.org/how-ransomware-spreads-and-works.php
[6]https://blog.malwarebytes.com/cybercrime/.../how-did-wannacry-ransomware-spread
[7]https://www.safaribooksonline.com/library/view/ransomware/.../ch01.html
[8] https://www.coursehero.com › ... › CYBER SECU › CYBER SECU 101
[9]https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
[10]https://in.norton.com/ransomware/article
[11]http://www.express.co.uk/life-style/science-technology/822033/cyber-attack-ransomware-how-to-protect-yourself-Petya-Wannacry-virus-antivirus
[12] http://blog.trendmicro.com/trendlabs-security-intelligence/massive-wannacrywcry-ransomware-attack-hits-
[13]https://www.albawaba.com/business/uae-saudi-arabia-most-targeted-countries-ransomware-mea-report-974222variouscountries
[14]https://www.timesofisrael.com/cyber-chaos-may-grow-as-workweek-begins/
[15]https://www.voanews.com/a/global-cyberattack-ransomware-national-security-agency-wannacry/3850424.html