Inside this Issue Vol 1:Issue 5/18

IFIS
Institute of Forensics & ICT Security
Forensics. Security. Training

With practical skills, You succeed

Forensics & Cyber Security Newsletter

Institute of Forensics and IT Security www.forensicinstitute.org

2ND ANNUAL CYBER SECURITY & RISK MANAGEMENT CONFERENCE 2018

#BEYOND CYBER SECURITY

Are you ready for the new era?

Don't miss the 2nd Annual Cyber Security and Risk management Conference 2018 #CSRM18 scheduled for
17th - 19th October, 2018 at Imperial Royale Hotel Kampala.

Register here now: https://forensicsinstitute.org/csrm18/

Cyber threats in 2018: Stay alert

Cybersecurity - what's going to happen next? Everyone wants to know, and no one can know for certain, despite armies of analysts and datacenters of machine intelligence. As we enter the 2nd half of this year, it behooves the Institute of Forensics and ICT Security (IFIS) to alert you about the cyber-attacks that may happen before the end of the year.

Supply Chain attacks

A supply chain attack is one in which attackers compromise a small software provider that operates in the supply chain of a much larger company that operates in another supply chain with tens of thousands of enterprises, using that access to surreptitiously compromise whatever enterprises lie downstream.

Supply chain security was and still is something many people don't know about. It came into force in 2017 when attackers compromised the update server for a popular Ukrainian tax software called M.E. Doc. The attackers sent out poisoned updates that infected endpoints with a wormable destructive malware that then spread itself around compromised networks. This ended up being the biggest story of the year: the so-called NotPetya (also known as contained a Trojan backdoor, were signed using a valid certificate, giving users false confidence that the software they were using was secure.

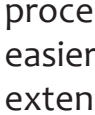
Security Tip:

Be aware of the potential risk of using software or hardware from organizations that do not have a responsible security stance. Look for vendors that issue CVEs, are quick to address vulnerabilities, and consistently strive to ensure that their built systems can't be compromised. In addition, take time to scan new software before downloading it to verify that it doesn't contain malware.

Malware Attacks

In 2017, adversaries took ransomware to a new level. Although malware attacks had been anticipated and prepared for, the level of sophistication used by the attackers was far higher than expected.

In May 2017, WannaCry-a ransomware crypto worm emerged and spread like wildfire across the Internet. To propagate, it took advantage of a Microsoft Windows security vulnerability called EternalBlue, which was leaked by the hacker group Shadow Brokers in mid-April 2017. WannaCry encrypts the computer's data, then attempts to exploit the vulnerabilities to spread out to random computers on the Internet and to computers on the same network. It would then display a message informing the user that files have been encrypted, and demanded a payment of around $300 in bitcoin within three days, or $600 within seven days. WannaCry had earned more than US$143,000 through bitcoin payments at the point the wallets were cashed out.



"Although malware attacks had been anticipated and prepared for, the level of sophistication used by the attackers was far higher than expected."

Experts predict that this kind of ransomware attacks will continue and computer users are urged to remain vigilant.

Security Tip:

Organizations should apply basic security best practices such as patching vulnerabilities, establishing appropriate processes and policies for incident response, and employing network segmentation.

Software Development Kits (SDK) attacks

It is very likely that attackers will try to compromise third-party software libraries and software development kits. Software and application developers increasingly rely on these tools and open source code sharing repositories, as they streamline the development process while also making it easier for individuals without extensive programming backgrounds to develop and distribute software.

These repositories, libraries and development tools can provide a one-stop-shop for attackers looking to quietly compromise a wide group of

victims. If one of these SDKs flawed or compromised, any application that incorporates it could be affected. Because so many applications rely on these libraries, attackers can broadcast their malware with only one successful attack that implants malicious code into the third-party library. This has already happened in at least two instances where attackers distributed malicious code into iOS and Android development libraries and the applications that incorporate them.

Security Tip:

Only use official SDKs supplied by the genuine distributor. Avoid downloading SDKs from random sites and torrents that are not affiliated with the SDK Distributor.

"It is very likely that attackers will try to compromise third-party software librariesand software development kits. ."

Social Media Tax: The Rise of VPNS

What is a VPN?

Basically, a VPN creates a virtual encrypted tunnel between you and a remote server which is operated by a VPN service. All your external internet traffic is routed through this tunnel, so your data is secure from meddlesome eyes.

How VPNs work

When you connect to a VPN, all the data that gets sent from your device to the private network at the other end is encapsulated. Each packet of data gets put inside another packet. Imagine putting a letter into an envelope to keep its contents from being read during transport. The envelope could still be opened, though and so with a VPN connection, encryption is the tamper-proof tape or glue on that envelope. Your Internet Service provider (ISP) can see the envelope but cannot see its contents and that's why they cannot stop you from accessing social media even if you have not paid the tax.

When the VPN connection is active, your computer/ smartphone appears to have the IP address of the VPN server, masking your identity. When your data reaches the VPN server, it exits onto the public internet.

"When you connect to a VPN, all the data that gets sent from your device to the private network at the other end is encapsulated."

"Basically, a VPN creates a virtual encrypted tunnel between you and a remote server which is operated by a VPN service."

Why use VPNS?

Even before the social media tax was introduced, many tech savvy and privacy conscious Ugandans were already using VPNs. This is due to a number of reasons. ISPs have been accused of collecting data from unsuspecting internet users without authorization. Due to the fact that all your online activity leaves a trail, ISPs can use this data to your disadvantage at a given time or another. ISPs are the ultimate data collection tools as one does not have many choices to choose from. For an average Ugandan, the affordable ISP choices are less than five.

While it is true that companies like Google and Facebook make money off your behavior online, you are not forced to use those services. If you someday woke up and suddenly decided to stop using Facebook, you might miss out people trying to show you which places they have visited and political rants, but you could still live a decent, possibly better, life. You could even choose to avoid the Google-o-sphere entirely by using the privacy conscious DuckDuckGo for your web searches, or drop the Google backed Chrome for the non-profit Firefox. This availability of options however is not the case with ISPs as they are few and among those few, the reliable ones are even fewer.

Additionally, because your data is encrypted, using a VPN will prevent many forms of Man in the Middle attacks, in which adversaries attempt to intercept your data en route. This is particularly true when using public/open Wi-Fi hotspots, which present a major danger to Internet users.

Furthermore, your IP address is hidden from the Internet because the VPN server acts as a proxy. Therefore, malicious websites and suchlike can only record the IP address of your VPN server, not your real IP address.

Drawbacks to using VPNs

One of the main disadvantages of using VPN is that it may slow down your Internet connection and consume more data. This is due to both the additional processing power required to encrypt and decrypt data and the routing of data through a third party server.

4th floor Ntinda Complex, Plot 33
Ntinda Road, Opposite St. Luke COU
P.O Box 40292, Kampala Uganda

admissions@forensics insitute.org
+256 414 231 36 / +256 393 517 236

Visit our website

www. forensicinstitute.org
www.summitcl.com

Send your comments on the articles or any other contributions to **risk@summitcl.com**

Our partners

summit consulting

The institute of Forensics & IT Security (IFIS) is a training arm of Summit Consulting Limited. We offer digital forensics, advisory and IT Security