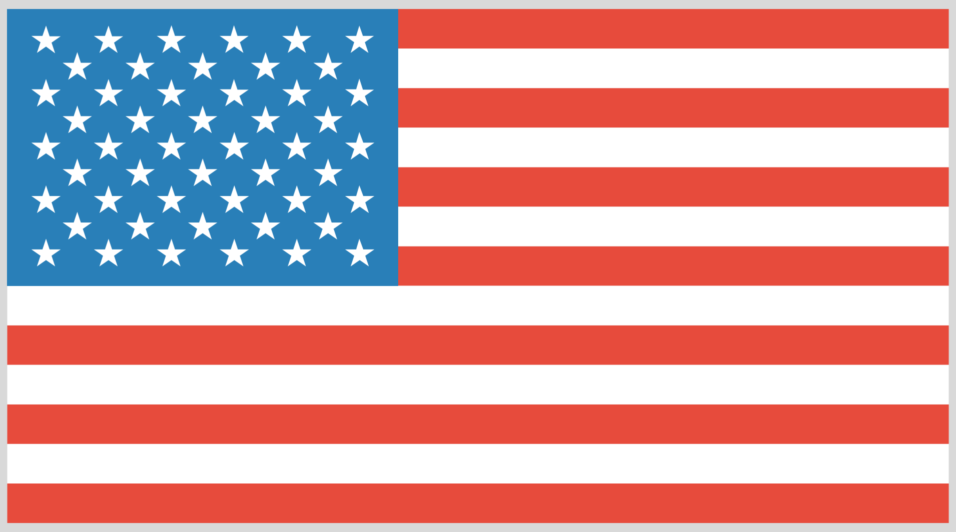
TECHNOLOGY TIMES

"Insider Tips To Make Your Business Run Faster, Easier And More Profitably"

KAMIND®

WHAT'S NEW

From our team here at **KAMIND IT**, we'd like to wish everyone a happy and safe **Fourth of July!**



Microsoft has released a new product called Azure Sentinel that alerts you to security incidents on all your devices (known as security incident endpoint management - or SIEM). We are automatically deploying this feature to all clients that have one of our security plans (Shield, Armor and Fortress).

JULY 2019

This monthly publication is provided courtesy of Matt Katzer, CEO of **KAMIND IT**

Our Mission: "We help our clients solve business problems with the use of The Microsoft Intelligent Cloud"

What Do Cybercriminals Really Look Like?

Cybercriminal organizations compete with each other for customers, fight for the best project managers and even look for leaders who serve in a CEO-like role to help them stay organized and on the task of stealing your money.

Researchers from IBM and Google described how cybercriminal groups operate, and often mimic the behavior of companies, including the one you might work for.

"We can see the discipline they have, we can see that they are active during office hours, they take the weekends off, they work regular hours, they take holidays," said Caleb Barlow, head of threat intelligence for IBM Security.

"It varies by groups. In organized crime, there is certainly a boss, much like you would hire a home contractor. That person doesn't necessarily do all the work. They hire the subcontractors, like the plumber and the electrician, that is typically how you do the work, you have lots of subcontractors."

Understanding how malicious hackers are able to structure their business operations is important, he said, so companies can better grasp what they're fighting, as the underground economy often functions in parallel with the broader economy.

Cybercriminal organizations aren't all the same, but a typical structure looks like this: a leader, like a CEO, oversees the broader goals of the organization. He or she helps hire and lead a series of "project managers," who execute different parts of each cyberattack, explains Christopher Scott, who leads the response to security incidents as part of IBM's X-Force business.

If the goal of the group is to get money by hacking a company and stealing its information, a series of project

Continued Page 2

Continued From Page. 1

managers will oversee different functions over the scope of the crime that play to their specializations. Specialists in malicious software might start by buying or tweaking a custom product to steal the exact kind of information the group requires. Another specialist might work to send fraudulent emails to deliver the malicious software to targeted companies. Once the software is successfully delivered, a third specialist might work to expand the group's access within the targeted corporation, and seek the specific information the group hopes to sell on the black market. In this case, an attack against a Fortune 500 company meant to steal and destroy data, the different colors roughly represent different job functions, Scott explained.

On the left of the graphic, attackers who specialized in compromising corporate networks worked their way into the business to gain a foothold. Other "project managers" compromised various employee accounts by stealing their credentials, and used those accounts to execute different tasks in the scheme, from gaining access to sensitive areas or gathering information.

Gaps across the timeline represent periods where the hackers stopped doing some of their activities so they wouldn't trip sensors the company used to detect criminal activity.

At the end of the 120-day cycle, other specialists, represented in bright red, came in to finish the job, using different malicious code to destroy their tracks as well as the company's data.Criminal groups don't exist in a vacuum. The offer what essentially are B2B services to one another and also hijack one another's progress -- just like the corporate world, explained Juan Andres Guerrero-Saade, who heads research at Chronicle, the Alphabet "Other Bet" company focused on cybersecurity.

"The sheer scale of organised cybercrime was shown earlier this year when hackers stole an estimated $1bn from more than 100 banks"

"If I'm a good developer, then I will create the ransomware and sell it, or sell it as a service," just like legitimate companies that offer software-as-a-service, said Guerrero-Saade. "I will then maintain the malware and if you find victims and get them infected and get them to pay, I will take 10% or 20%." Some of these service providers have seen their earnings cut back in recent years. In the first half of this decade, a type of malicious software known as banking trojans, which steal a person's credentials to take money from their bank account, became popular. Specialists who offered money-laundering services were in high demand. That demand has waned in recent years as ransomware grew more popular and criminals were able to get money directly. This is common among specialists who offer distributed denial of service (DDoS) attacks, which work to overwhelm a victim company's computers with so much information that they shut down. Companies are getting better at identifying the hallmarks of many of these different types of criminal-business structures said Scott. But sometimes, they grow so big and so organized that they become too easy to identify -- and thus, go out of business. "When you are dealing with these more bureaucratic type organizations, the activities are very predictable," he said.

Understanding these trends is important for companies hoping to fight cybercriminals, Scott said. "If you are chasing a particular adversary, you may actually get to understand how many of the same tools, techniques and practices they use. [Companies] don't have unlimited funds, but if you know the tactics properly, you can really focus the security spend."

Kate Fazzini, CNBC
May, 2019

Shiny New Gadget of The Month

GoPro HERO7 Black Action Camera

The HERO7 Black by GoPro is sleek, compact, easy to operate, and better-connected than any of its competitors. It can capture 4K video at a barely believable 60 frames per second — a tall task for any DSLR out there.

Most importantly, the HERO7 Black has the best stabilization tech in its class, ensuring that all your adventures will be captured with amazing detail.
It also has the capability to shoot bursts of 12 MP images. The HERO7 Black can go up to 33 feet underwater without a housing.

Freakishly smooth footage. Smart-capture superpowers. Battle-tested and waterproof without a housing. This is HERO7 Black, the most advanced GoPro ever. With HyperSmooth stabilization, you'll get gimbal like video— without the gimbal. A new intelligent photo mode delivers the best, most brilliant images automatically. And now with live streaming and the GoPro app, you can share every amazing moment as you live it. HERO7 Black takes GoPro performance —and your photos and videos—to a whole new level.

Cyber and the Healthcare Industry

The Healthcare industry has featured in the top 5 industries attacked by cyber criminals for a number of years now. The WannaCry ransomware attack earlier this year that affected many health trusts across England and Scotland brought the health impact of the cyber threat to the forefront of media and political debate in the run up to the 2018 General Election. So why would anyone want to attack healthcare and what are the threats? 2018 was a very difficult year for healthcare when it came to cyber-attacks and developing cyber threats. According to the TrapX Security 2018 Healthcare Cyber Breach Research report, "the nature of the threat continues to diversify into a greater variety of complex attacks promoted by sophisticated and persistent human attackers. These attacks against hospitals and medical organisations are still driven by the lucrative economic rewards for organised crime. Medical records are among the most complete set of records available and, hence, are in demand for a variety of reasons."
In October 2017 Ben Gummer, Minister for the Cabinet Office and Paymaster General warned that the NHS was at risk of cyber-attacks, saying that "hacking is "no longer the stuff of spy thrillers and action movies" but a clear and present threat and large quantities of sensitive data held by the NHS and the Government is being targeted by hackers."
In January 2017 Barts Health Trust warn its staff that the trust's four hospitals in East London: The Royal London, St Bartholomew's, Whipps Cross and Newham were experiencing a "ransomware virus attack." This came after similar attacks on Northern Lincolnshire and Goole Foundation trust in the previous October. A report on the Deep Web black market for electronic health records (EHRs) by researchers affiliated with the Institute for Critical Infrastructure Technology pointed out that "healthcare systems are relentlessly and incessantly attacked by different types of attackers." One of the reasons that medical networks remain vulnerable is that many legacy systems and devices lack the ability to be updated and patched, yet are connected to networks. Or the updating of systems, often via patches provided free from operating system vendors, is not seen as a priority by senior managers and something "IT are responsible for". It therefore doesn't matter if the newer devices are completely up to date as the organisation's "Internet of Medical Things (IoMT)" becomes vulnerable to its weakest link. Medical records, especially but not exclusively in the USA, by dint of their comprehensive nature, sell for hundreds of dollars on the Dark Web and there is no shortage of them. According to the IB Times last year, a hacker claimed to have broken into multiple Heathcare Datas Centers across America and listed a fresh trove of 9.2m records on a Dark Web based marketplace for 750 bitcoin (£368,000). The vendor, using the pseudonym 'The Dark Overlord', claims the plaintext 2GB database includes names, addresses, emails, phone numbers, date of births and Social Security Numbers (SSNs) belonging to 9,278,352 Americans. However, for those compromised, many don't realise that their records can be sold repeatedly by the criminal networks operating in the Dark Web and that this could cause long term problems. Information that is contained in medical records can be used for many different types of identity fraud and phishing attacks and because of its comprehensive nature, the threat from these can persist for many years.
In the UK, the attack vector seems to be different to the USA and attacks are mainly via ransomware. Trying to extort money from vulnerable hospital trusts rather than individuals. NHS hospital trusts in England reported 55 cyber-attacks in 2016, according to data obtained by the BBC from NHS Digital, who oversees cyber security. The WannaCry attack blew this statistic away and put a spotlight on cyber security across healthcare in the UK. As the attack unfolded, Eugene Kaspersky from Kaspersky Labs said that it, "looks like a cyberattack of a criminal nature but with a global impact that's very close to terrorism." Kaspersky continue to help Europol to try and track the perpetrators. Until now, NHS Digital reported a steady increase in reporting but were quick to point out that this increase didn't necessarily mean an increased number of attacks, just better awareness and they didn't believe any patient records had been compromised. Oliver Farnan, from the Oxford Cyber Security Centre, said ransomware attacks had become more common and 'The risk is going to increase'; how right he has been.

UK Security Expo team
December, 2018

Exposed database reveals personal information of 1.6 million job seekers

An unsecured database of personal information, including phone numbers, salary expectations and openness to new job opportunities, of about 1.6 million job seekers from around the world has been discovered online, according to research published Monday. The database, found by independent researcher Anurag Sen in May, includes information on professionals from the US, Australia, Japan and several other countries.

The database appears to be owned by Indian recruitment company Talanton AI. It's hosted in plain text on a cloud server, and anyone with a web browser can access it with the right web address.

Names in the database include potential job seekers with high-profile roles in the Australian government, at Tommy Hilfiger Japan and in the FBI's Domestic Security Alliance Council, a public-private partnership that shares information about cybersecurity threats with the government.

Sen released the research as a contractor for Safety Detective, an Israeli company that reviews antivirus software. A researcher at Safety Detective who helped vet the information said the exposure could put workers in an awkward position at their jobs. What's more, phone numbers and email addresses can help scammers who want to impersonate company officials.

The data appears to have been found on LinkedIn profiles, as well as with direct outreach to job seekers. Safety Detective checked some of the information and determined it was real. The exposure is an example of a serious, ongoing problem that can inadvertently affect almost anyone. Companies around the globe have moved sensitive information to cloud servers, but many lack the expertise to do so securely. The transition has led to exposures of sensitive health information, financial data and private contact information. Even children's information has been exposed. A database exposure is not the same as a hack, because you don't need to break into a computer system to find the data. Instead, you just need to find the right IP address, which is the distinct numerical address assigned to each page on the internet. There's no indication hackers have accessed the information in the Talanton AI database.

In May, Sen found an unsecured database owned by Indian marketing company Chttrbox, which contained contact information for Instagram influencers. The data wasn't private, but had been collected in a manner that violated Instagram's terms of service, according to the photo-sharing service.

A community of researchers around the world spend their time hunting down exposed databases and trying to get them fixed, but new databases with poor security come online every day, experts say.

Talanton AI's website doesn't appear to be fully functional. Links and buttons on the home page lead to 404 error messages or do nothing. When contacted about the exposure, a Talanton representative said he would share the information with the appropriate person.

The database is hosted on a cloud server operated by Tata Communications. It isn't the responsibility of a cloud service provider to secure client information, but some will notify customers if a problem is discovered and will help protect the data.

Tata said it's investigating the exposed database, according to Sen. Tata didn't respond to requests for comment from CNET.

Laura Hautala
June, 2019

Security firm Cellebrite says it can unlock any iPhone

Apple continued its security push this month during its WWDC event, where the iPhone maker unveiled new iOS features designed to keep your data private. One security company, however, says it can unlock all Apple devices and extract the data.

Israel-based company Cellebrite says on its website that it can "bypass or determine locks and perform a full file system extraction on any iOS device." The company offers support for Apple devices running iOS 7 to iOS 12.3, which the iPhone maker released in September.

Cellebrite also says it can do a physical or full file system extraction from high-end Android devices from Samsung, Motorola, Huawei, LG and Xiamoi.

Cellebrite made news in 2018 when reports came in that the company, which works with US law enforcement agencies including the FBI and ICE, could unlock some Apple devices.

Back in 2016, Apple and the FBI were in a legal battle over the iPhone maker's refusal to unlock an iPhone 5C used by a shooter in the 2015 terrorist attack in San Bernardino, California. The law enforcement agency was able to unlock the iPhone thanks to a third party, which some reports say was Cellebrite.

Cellebrite didn't immediately respond to a request for comment. Apple didn't immediately respond.

Oscar Gonzalez
June, 2019

Who Else Wants To Win A $25 Gift Card?

Congratulate **Dennis Warneke of Lake Oswego**, last month's trivia winner! You can be the Grand Prize Winner of this month's Trivia Challenge Quiz! Just be the first person to correctly answer this month's trivia question and receive a $25 Amazon Gift Card! Email your answers to **trivia@kamind.com**

Under which tab do you find the Microsoft 365 Comparison Chart at www.kamind.com?

A. Licensing Drop Down Tab
B. Microsoft Azure Tab
C. Services Tab
D. Licensing Portal

amazon