APT28 Targets Financial markets: zero day hashes released

root9B

"In the last year alone Russian hackers have reportedly stolen up to 900 million dollars from banks around the world."

May 10, 2015

root9B: The Threat Defiance Report

APT28 TARGETS FINANCIAL MARKETS

ROOT9B RELEASES ZERO DAY HASHES

Cybersecurity experts are increasingly concerned about the threat posed by Russian hacking groups. Besides well-known events such as the attacks against Estonia, Georgia, and Ukraine; recent headlines have seen Russian hacking syndicates credited with targeting NATO officials at conferences, stealing hundreds of millions from banks, and successfully penetrating the White House unclassified computer network. The increase in cyber-exploits is also accompanied by a much more aggressive Russian foreign policy, which has seen them invade Ukraine and literally seize control of sovereign territory in Crimea. So it should not surprise anyone that just as nuclear capable Russian bombers are increasingly penetrating foreign airspace, their cyber-warriors appear to be ramping up their intrusions as well. But this time, perhaps for the first time, root9B has managed to find where they were hiding and identified effective defenses against their intended attacks. This is what happened in late April and early May of this year.

Our firm of cybersecurity experts, staffed by veterans from the United States Department of Defense, identified suspicious activity within one of our client's networks; a threat which on closer inspection bore the unique signature of a group of Russian hackers well-known in the cyber-security industry. As Cyber Threat analysts continued to follow the indicators, they uncovered a global attack in the making, and took steps to protect not only our clients, but other identified victims as well.

Sofacy, Sednit, Sourface, APT-28, and a host of other names are all used to describe this particularly prolific and superbly talented group of Russian hackers, which has strongly suspected ties to Russian intelligence services. In the last year alone Russian hackers have reportedly stolen up to 900 million dollars from banks around the world. Over the past three to five years they have built the largest botnets ever discovered, and stolen the log-in and password credentials to literally

tens of millions of online accounts. Well known for their ability to infiltrate and remain undiscovered in networks for long periods of time, they may be the most successful group of hackers in the world. Whereas previous attacks have been attributed and analyzed only after they have run their course, this was the first and only known Sofacy attack to be discovered, identified, and reported – all before it could even begin! The analysts and tools that enabled this to happen are unique and proprietary. This report documents the first ever operation to use threat intelligence and adversary tactics to discover and reveal the prepositioning of Sofacy zero-day malware. This document also includes the reporting of previously unknown malware indicators and hashes.

The Threat

Russian President Vladimir Putin recently described the Internet as "an invention of the CIA." But the group most widely associated with his government dominates the world of industrial scale hacking. First discovered circa 2007 using security vulnerabilities in Microsoft Windows, Sofacy has gone on to develop and launch truly enormous attacks exploiting numerous applications including Adobe's Acrobat, Microsoft Excel, and others. Some attacks have focused on the sorts of targets that seem likely to be of interest to Russian intelligence services. NATO, defense industry corporations, and government domains of states opposed to Russia on various issues have all been, at times, victims of Sofacy. At other times large banks and private corporations have been hit hard by Sofacy exploits, at a cost of hundreds of millions to the victims. Sofacy's choice of targets has historically been an interesting mixture that has fueled an ongoing debate over whether the group is criminal in nature, or actually an agent of a nation-state. Most cybersecurity analysts have concluded that the group's affiliation with the Russian government is undeniable. But there are detractors. Those who argue loudest against such assertions cite Sofacy's prolific criminal profit as evidence that they are most likely not agents of the Federal Security Service (FSB); while others suppose that the crimes committed bearing Sofacy's unique signatures is a perfect cover behind which the Russian Government prefers to remain.

The Defenders

Started in 2012 and staffed almost entirely by former United States Department of Defense civilians and military cyber-warriors, root9B brings a unique base of knowledge and experience to the task of securing corporate networks. This comes at a time when the demand for services is stronger than ever and increasing daily. Calling on years of collective experience in positions that placed their analysts at the tip of the cyber-spear, root9B has developed a unique approach to the problem of cyber-defense. Understanding that the present tools are failing at an alarming rate, they have developed methods and software applications which seek to augment, rather than replace, existing cyber-security defenses. The problem is not that traditional methods do not work. It is that hackers are becoming increasingly sophisticated and able to generate new threats faster than ever before. Standard network security systems typically fail against what are known as "zero-day threats." Zero-day is a term that refers to a new kind of hacking exploit that has never been seen before, and is therefore not detected by standard virus and intrusion detection software. Typically, such threats take an alarmingly long time to detect and eliminate, often more than a year. They were once relatively rare, because it takes a high degree of skill to develop and exploit them. The production and sale on the black market has increased exponentially in recent years, developing into a criminal industry that is placing online commerce, as well as national security, at growing risk. In the time between deployment of a zero-day and its eventual discovery and eradication, corporations can suffer enormous losses without even realizing that the threat was ever there.

To combat threats, root9B realized that technology is not the problem. **"Computers don't attack networks. People do,"** said root9B. You cannot build a better system to stop a determined human, you must think like the attacker and provide manned cyber defense operations as the new adaptive security posture. root9B operators and software developers designed

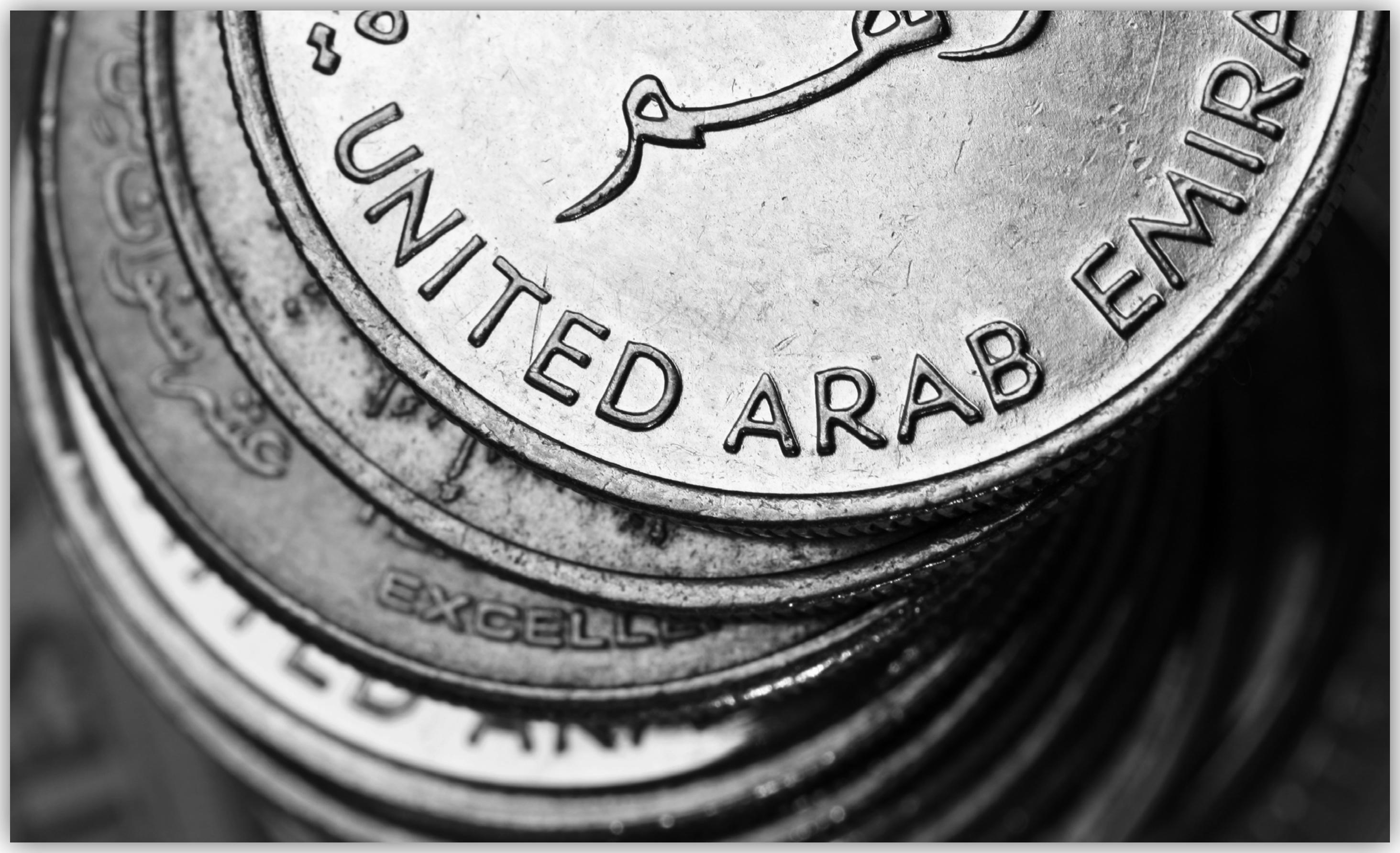
MANNED
INFORMATION
SECURITY
WE SEND SPECIALIZED CYBER OPERATORS INTO YOUR NETWORK TO
HUNT FOR AND STOP THE INTRUDERS YOUR EXISTING SOLUTIONS ARE NO MATCH FOR.
root9B

and constructed proprietary methods of discovering and dealing with adversaries. With a network defense strategy of pursuit and deterrence in mind, root9B operators conduct Active Adversary Pursuit (HUNT) operations as a tailored solution for cyber security teams. Working in concert with traditional network defense appliances that currently reside in our client's proprietary network, root9B's HUNT platform delivers a pro-active defense protection capability to identify, pursue, and mitigate cyber threats. This approach was developed by root9B in order to leverage previously existing security products with client-specific threat intelligence and proprietary capabilities that can identify sophisticated vulnerabilities, generate actionable intelligence, and install solutions with much greater speed and efficiency.

Winning In Advance

During the end of April 2015, root9B analysts were conducting routine security analysis to explore and discover new and emerging cyber threats. Threat Analysts discovered what appeared to be a targeted spearfishing domain aimed at a financial institution. The server it was found on raised even more questions, because although security experts knew the server as a bad actor, it was generally associated with malware used in nation state attacks. As analysts continued their work they discovered several more pieces of new malware. The malicious code bore specific signatures that have historically been unique to only one organization, Sofacy. This malware was pointing at a spearfishing domain registered to impersonate a Middle Eastern financial institution and the domain registration details did not match normal Sofacy operational signatures. That said, the malicious software certainly did. Members of root9B's operations team conducted HUNT operations, remotely deploying their live memory capability across the clients proprietary networks to analyze known techniques that can evade the most efficient security products on the market. root9B's capability parses live memory while the system is running and looks for indicators of advanced tactics such as code injection or security product bypassing. Using a combination of standard industry tools and proprietary techniques our analysts began to develop a larger picture of what was taking place. Immediately, root9B identified that preparations were being made for a larger scale attack similar to previous Sofacy attributed exploits, and the attack was still in the preparatory stages. To our analysts, this was a rare opportunity. "It is rare enough to learn of an attack of this potential magnitude in advance, but to have all of the information necessary to stop it before it begins is unprecedented,“ said an unnamed root9B analyst.

Evidence of intrusion within client networks pointed to a specific server, CARBON2U.COM, that had been previously linked to malicious activity and identified by other security firms as part of the infrastructure utilized by the Sofacy group. Analysts studied the remaining domains registered on that server, and initially noted that one in particular, CBIUAEBANK.



COM, appeared to be a fake version of CBIUAE.COM, the actual domain of the website of Commercial Bank International of the United Arab Emirates. Further analysis lead to even more suspicion, and those suspicions grew even stronger as they watched another comparable domain created, CBIUAEBN.COM. As analysts passively monitored CARBON2U.COM, they observed as the apparent fake domains they were monitoring migrated to other servers; first to SITE4NOW.NET and later to OK2HOST.COM. This gave analysts two more suspicious servers to study, and added considerable data analysis.

root9B analysts began to dissect the data at hand to identify common tactics, techniques, and procedures used by the adversaries which could provide further information about the planned hack, including information about potential attack vectors. As root9B analyzed increasing amounts of metadata and associated indicators, they were able to identify a very unique signature consistently used by someone involved in setting up the hack. Investigating the apparently fictitious list of personas used to create and register domains, a pattern emerged. Due to the nature of this unique signature, root9B is in the process of further documenting and reporting to the proper authorities.

The discovery of the hacker's single mistake in tradecraft was indeed a powerful catalyst, and lead to the discovery of a treasure trove of new indicators. The new discoveries included evidence related to past attempts to launch attacks against many of the same targets, including the aforementioned Commercial Bank International. What the analysts eventually had was a very detailed view of the specific tactics employed by this adversary; and a window into a plan for a hack that was even larger than originally believed, much larger. Where initially they had only a single fake domain pointed at CBI, now there were six additional domains, all used to target this single victim. Many of the fake domains appeared to have been created by several of the same accounts, and open source analysis indicated that the names listed for the person registering the addresses was clearly fictitious; probably chosen at random from the Internet.

The analysts at root9B understand better than anyone the significance of this analysis. As far as any of them know, and it stands to reason that they would, there has never been a case of a large-scale attack utilizing numerous zero-day exploits that were so thoroughly mapped in advance before. The analysts who worked this case now understand that the attackers began preparations for this campaign in June 2014, a full eleven months ago. The design of the hack bears striking similarity to the very exploits that have made Sofacy so feared and respected. At least nine months of meticulous preparation coupled with one slip of tradecraft has enabled root9B to inform potential targets prior to the execution of the strategy.

With the exception of CBIUAEONLINE.COM, there are numerous consistencies amongst the tactics employed by the hackers. The group generates what are likely fictitious personalities as the "owners" of each of the fake domains. All of the fictitious personalities list the same street address. While they change names and house numbers for them, they all reside on Cloverdale Lane in DeSoto, Texas. Analysts noting the similarity did not have to visit the street to determine that it was unlikely that they each resided in different homes on the same street. In fact, even the house numbers changed only slightly from one domain to the other. In addition to the links between the addresses, streets, and names, they found that the registrant phone numbers were also very closely related. The only differences in registrant data from one domain to the next involved very slight modifications to the country codes or by changing the third digit. This kind of flaw in tradecraft allowed for further detailed network analysis.

Further analysis of the street addresses enabled root9B to correlate the address and personas listed as registrants via public records, doing so showed that most of these addresses did not even exist, and the few addresses confirmed to physically exist did not have residents with the names listed. This became a key signature of the hackers; a common thread which unraveled all of Sofacy's careful preparation. Often those wanting to generate a free and anonymous email address will use a false name and address in order to conceal and preserve their true identity.

The information below dictates open source research on the adversary's creation of domains. As previously noted, root9B is in the process of further documenting and reporting probable fictitious personas to the authorities.

DOMAIN: CBIBUAE.COM

- Created: 2014-06-14
- Nameserver: nvhserver.com

DOMAIN: CBIUAEONLINE.COM

- Created: 2014-06-24
- Updated: 2014-07-03
- Nameserver:aspnix.com (suspended-domain)

DOMAIN: ROYALBSUK.COM

- Created: 2014-07-02
- Updated: 2014-07-06
- Nameserver: (suspended-domain)

DOMAIN: CIBUAEONLINE.COM

- Created: 2014-11-27
- Updated: 2014-01-27
- Nameserver: hostzeal.com

DOMAIN: CIBUAEONLINEBN.COM

- Created: 2014-11-28
- Updated: 2014-01-27
- Nameserver: site4now.net

DOMAIN: CBIUAEONLINE.COM

- Created: 2014-12-10
- Updated: 2014-02-08
- Nameserver: ok2host.com

DOMAIN: CBIUAEBANK.COM

- Created: 2015-04-29
- Updated: 2015-05-02
- Nameserver: site4now.net

DOMAIN: CBIUAEBN.COM

- Created: 2015-04-29
- Updated: 2015-05-03
- Nameserver: ok2host.com

Correlating the increasing amounts of information, root9B analysts have determined that the adversary responsible for the initial attack in June 2014 was almost certainly the same, or very closely-related to the entity responsible for creating at least two of the domains in April 2015. The same person was ostensibly responsible for registering the two most recent domains (CBIUAEBN.COM and CBIUAEBANK.COM). Analysts from root9B now believe that the adversary most likely selected this name through an internet search, and that these personas, while possibly real names, are not the true names of those individuals associated with the preparations for this attack.

root9B analysts have also identified an additional persona; one that did not appear to directly relate to this attack against CBI UAE Bank, but that carried similar operational tactics to include comparable street address schemes and the registration of domains closely resembling financial institutions. By studying the new persona, root9B discovered they had previously created several domains and websites, all of which have been flagged as Fake Financial Institutions by security analysts. Also identified during this analysis, was the prepositioning of a domain targeting the financial institution B-OF-AMERIC.COM, created in April 2015. This indicates that Bank of America, is among the probable targets.

This same individual has registered numerous other fake domains on many more name servers. One of these name servers, BULKBREAKERS.COM, contains several other international financial institutions. One of those domains, T-D-CANADATRUST.COM, was updated on 23 March 2015, and appears to be targeting Toronto Dominion (TD) Canada Trust. Among the apparent targets of other domains similarly created or updated in 2015 are: the United Nations, United Nations Children's Fund, United Bank for Africa, Regions Bank, and possibly Commerzbank.

Results

While root9B's discovery began with servicing their own customers, their analysis has revealed an adversary pattern that has enabled the identification of previously unknown target vectors. As root9B analysts continued to peel back the layers, it became more apparent, that this attack was likely associated with Russian intelligence. The targets included multiple major financial institutions, as well as the international government domain. In addition to identifying targets, root9B analysts also discovered indicators of malware, the analysis of which revealed several zero-day threats and their corresponding "hashes." Each new discovery revealed more information, enabling a more complete picture to emerge. root9B discovered and analyzed numerous other domains being staged or recently created for the malicious cyber operation. Also discovered was a fatal flaw in the hackers tradecraft that lead to a major breakthrough. Research based on the adversary's flaw in tactics showed that there was a strong likelihood of two distinct subgroups, each of which utilized unique

methods of cover for their activity. Each of the two groups also had a unique theme to their target sets. The first seemed to focus on military, diplomatic, and media targets, and relied on the cover of proxies and private domain registrations. As documented earlier, the other group used deliberately falsified personalities, all of which claimed to be American citizens, and focused on financial and banking targets. Understanding the scope of the newly staged malicious operations, root9B also tipped the information to the appropriate international and domestic government authorities.

While the continued vector of the attack remains unclear, root9B assesses that it will most likely be a spear-phishing campaign. This attack vector will likely use a well-crafted email containing either a malicious file or web hyperlink to what recipients believe is the actual website; but is instead a fake landing page. In typical attacks of this nature, once users navigate to the link, visitors are prompted to supply account credentials and personal information under the false assumption that they are communicating with their bank via a secure link. However, it is possible, that the Sofacy group could utilize this server as a vector to deliver malicious code to the banking victims in an attempt to obtain access to the network. As of October 2014, the Symantec Corporation had reported an increased use of spear-phishing emails containing malware specifically targeted against financial institutions.

According to their conclusions, root9B analysts expect that spear-phishing attacks will begin in the near future, or may have already commenced. As root9B continues to work with authorities it is recommended that the aforementioned financial institutions take caution examining any and all correspondence. In addition, it is recommended that networks begin blocking the following hashes and communications with the identified Command and Control (C2) server:

Malware SHA1 Hash

0450aaf8ed309ca6baf303837701b5b23aac6f05

bb909d9c27a509bf97cdc85268556ff5a6d2550a

f325970fd24bb088f1befdae5788152329e26bf3

a351842ee01374d66bae35354ffe72f0b1b8a40b

Command and Control (C2) Server:

176.31.112.10

Interesting samples of over 250 identified malicious domains*:

b-of-americ.com
osce-military.org
bbcnewsweek.com
qov.hu.com
settings-yahoo.com
yovtube.co
googlesetting.com
cbiuaebn.com
cbiuaebank.com
techcruncln.com
un-unicef.org
royalbsuk.com
kwqx.us
middle-eastreview.org
unitednat.org
fbonlinelottery.com
fubnt.com
globeshippers.biz
globeshippers.net
gsandsc.com
gshippers.com
hesselawchambers.com
largefarm.net
regionsbnk.info
seatreasures.org
ssandsc.com
t-d-canadatrust.com
techielawfirms.com
togounoffice.com
ubagroupsgh.com
un-unicef.org
unicomba.com
universalcoba.com

*Some domains may have been previously reported as associated with the Sofacy Group. It is root9B's opinion that new information regarding cybercrime targeting banks makes this information relevant.

Footnotes:

[i] http://www.newsweek.com/2015/05/15/russias-greatest-weapon-may-be-its-hackers-328864.html

[ii] http://www.bloomberg.com/politics/articles/2014-10-30/security-firms-tie-russian-government-to-utilities-hacks

[iii] http://www.theguardian.com/world/2014/apr/24/vladimir-putin-web-breakup-internet-cia

[iv] http://www.bloomberg.com/politics/articles/2014-10-30/security-firms-tie-russian-government-to-utilities-hacks

root9B
102 N. Cascade Ave | Suite 220
Colorado Springs | CO | 80903
info@root9b.com
www.root9b.com

INNOVATION · EXCELLENCE
root9B
AMAT VICTORIA CURAM