NTT Security

GTIC Monthly Threat Report

July 2019

A Global Threat Intelligence Center
publication from NTT Security

Contents

Spotlight on Health Care: Insight into Attack Statistics

Lead Analyst: Jon Heimerl

"Your health is your real wealth." – Mahatma Gandhi

What is more private than your medical information?

Realistically, in the health care industry, the information available as part of your health care details isn't all just about your health. It includes payment information, which could be insurance, credit card numbers or even bank account numbers. It's also about your private information – social security number, driver's license, name, date of birth, address, and other information which describes "who you are."

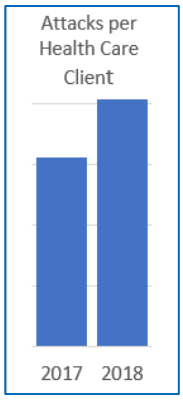
In the world of cybersecurity, the variety and depth of information available in your health record makes it a valuable commodity for attackers. The information supports theft and identity theft, and provides information which makes potential victims more vulnerable to social engineering and even blackmail.

Given the value of the available information, it might be surprising the health care industry is not consistently ranked as one of the most highly attacked industries. According to data from the NTT Security Global Threat Intelligence Report, health care ranked as the seventh most attacked industry globally, out of 18 industries analyzed.

Finance	17%
Technology	17%
Business and Professional Services	12%
Education	11%
Government	9%
Manufacturing	7%
Health Care	7%

Targeting Health Care Regionally

Regionally, the difference in attack volume and focus was pronounced. Health care was the fourth most attacked industry in the Americas, yet health care did not rank higher than the seventh in any other region. And despite their attack ranking, health care organizations accounted for over 15 percent of all incident response engagements – the second most common industry to obtain such services globally, behind only finance.



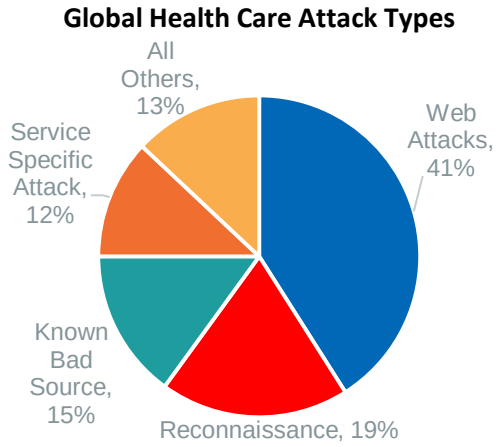
While the increase in attacks was more pronounced in the Americas, health care felt the impact globally as well. Analysis of global data on industry attacks over the past couple years, shows that the average health care client experienced a 31 percent increase in attack volume from 2017 to 2018. Health care organizations which might have experienced, for instance, 10 attacks a day in 2017 would experience 13 attacks per day in 2018. Organizations which may have experienced 100 attacks a day in 2017 would suddenly be facing 130 attacks per day a year later. This has created a demand on IT and security support within health care which is increasingly difficult to manage since *investment*

in security is not growing at the same rate. While some fluctuations in attacks are expected on a year-to-year basis, an increase of this magnitude should not be ignored and may indicate a trend towards attacks actively targeting health care organizations.

While some geographic areas observed small differences in attack sources, globally those sources were consistent. Worldwide, 62 percent of all attacks against health care organizations originated from the United States (U.S.) and Thailand. If you add China, Hong Kong, and Singapore, the top five attack sources account for nearly 77 percent of all attacks. That is a high concentration of attacks from a relatively limited variety of sources.

Profiling Technical Attacks

In every region, the most common attack types targeting health care organizations were web attacks, service-specific attacks, attacks from known bad sources, and reconnaissance activity. The order of these attacks varied in each geography, but the attack types remained consistent.



Web attacks are usually highly automated, and dominated attacks in many industries throughout 2018. Health care was no exception, as, globally, web attacks made up 41 percent of all attacks against health care organizations. But, the characteristics of these attacks varied when considering the sources of those attacks.

- Attacks from the U.S. were characterized by DNS attacks, bot C&C traffic, and remote code execution attacks, among others.
- Attacks from China and Hong Kong included characteristics similar to attacks from the U.S., with the addition of SSH brute force attacks.
- Attacks from Thailand and Singapore were characterized by a variety of denial of service attacks, buffer overflows, and brute force password attempts, among others. It appears likely the hostile activity from Thailand and Singapore were related, since, not only did they share many of the same characteristics, but they targeted many of the same organizations.

Throughout June and July 2019, hostile activity directed at health care organizations continued to evolve. Brute force attacks dominated attack activity with over 50 percent of total activity. In addition, bot C&C traffic continues to be an issue for many health care organizations. Detections from malware and malware command and control has been common in health care, but for June and July 2019, over 99 percent of all malware activity was related to the Mowfote, Zegost, or DoublePulsar Trojans or the Ortega rootkit. The remaining hostile activity is dominated by web attacks, including SQL injection, cross-site scripting and code injection.

Most recently, exploit attempts directed at health care organizations have been surprisingly focused. Over 90 percent of all exploit attempts in June and July 2019 focused on the top five most targeted CVEs. The implication is that patching these five vulnerabilities has the potential to reduce exploit attempts directed at the organization by as much as 90 percent.

Vulnerability CVE	Technology	CVSS
CVE-2017-0171	Microsoft Windows Server 2016	4.3
CVE-2019-0708	Microsoft Windows 7	10.0
CVE-2016-3087	Apache Struts	7.5
CVE-2017-5638	Apache Struts	10.0
CVE-2017-12263	Cisco License Manager	5

Beyond the top five most targeted vulnerabilities, seven of the top 25 vulnerabilities targeted Microsoft Windows products or operating systems, and five of the top 25 vulnerabilities were related to Apache Struts. So, if an organization only focuses on these two technologies, they have the potential to remove 12 of the top 25 most targeted vulnerabilities from their environment.

The vulnerabilities also appear more focused if we consider vulnerabilities by the highest CVSS scores – such as those with scores over 9.0. The most attacked vulnerabilities in health care organizations include nine vulnerabilities with scores of 9.0 or higher – three from Microsoft, and three from Apache Struts – further reinforcing the need to patch these technologies.

Conclusions

The health care industry has always been an attractive target for attackers. Recent trends suggest attackers are increasing their level of focus on health care, consequently increasing the overall risk for any health care organization – and patient records. Attackers and attack techniques will continue to evolve, but as of June/July 2019 technical attacks against health care organizations have been focused on a relatively small number of patchable vulnerabilities.

Truly mitigating ongoing attacks requires a multi-level security program with a wide variety of overlapping technical and non-technical controls. But, focusing on these two recommendations is a start:

1. Prioritize patching – especially on critical and exposed systems, and especially for Microsoft and Apache Struts products.
2. Increase focus on active management of security programs. There is the strong potential that the 31 percent increase observed in attacks against health care organizations from 2017 to 2018 is a trend with suggests increased attacker focus.

For more information about attacks against the health care industry, download and read the 2019 NTT Security GTIR[1].

[1] https://www.nttsecurity.com/landing-pages/2019-gtir

Becoming Active on the Dark Web

Lead Analyst: Chris Schwartz

I am a threat researcher on the Dark Web.

When at war and facing an enemy, no words could be more accurate than Sun Tzu's "If you know neither the enemy nor yourself, you will succumb in every battle."

The logical question is "how does one begin to know the enemy?" The "easy" answer is to live their experiences. The harder part is actually navigating the Dark Web in a meaningful manner.

The internet itself – especially the Dark Web – represents the modern cyber-battlefield. The Dark Web is not a magical universe inhabited by evil. It is more like an extension of the modern internet, which you cannot navigate without specific software. And the Dark Web has sites, information, and marketplaces, some of which you cannot readily access unless you are explicitly invited.

But… the Dark Web is different enough that you can't just access it as easily as you can the open internet. It requires certain technologies and skills to access the best information. Being active on the Dark Web can increase your own risk if you are not careful about what you are doing.

The goal of this section and the referenced blog are not to make anyone experts in the Dark Web, but to help describe some of those rules, techniques and technologies which might expedite the learning process, from someone who is still going through that process.

A dramatic over-simplification on accessing the internet underground includes an introduction and the following first steps to consider:

1. Utilize TOR – or another Dark Web software suite – software commonly used on the Dark Web to help ensure all users and hosts are following a unified standard of encryption and anonymity.
2. Develop an alternate ego – a "sock puppet" – an online identity and persona used for the purposes of deception – so that your "sock puppet" is active on the Dark Web, not you.
3. Build a reputation based on that sock puppet – since you can't just walk right onto the deepest corners of the Dark Web. You need to make a name for yourself – gain a reputation – to get invited into the secret club.

The Dark Web includes some of the latest and most advanced cyber threats, tutorials, message boards, hacker tools, stolen data repositories, and other related information. Monitoring those spaces can greatly assist security researchers in staying ahead of the ever-changing threat landscape and planning of threat actors. If you can learn about the tools and techniques hostile threat actors are using, you have the opportunity to use that information to improve your own practices and controls. Simply being on the sites, observing the chatter, and recognizing the trends provides a more holistic view of the threat landscape.

Some readers may be well-versed in accessing and navigating the Dark Web; others may not. This is just a quick first look into what can happen on the Dark Web. For more details, read Becoming Active on the Dark Web [2]– the first in a blog series on the Dark Web.

[2] https://technical.nttsecurity.com/post/102foy9/becoming-active-on-the-dark-web

Monthly Observations: Malware

Lead Analyst: Terrance DeJesus

In July 2019, GTIC researchers took a closer look at malware observations regarding NTT Security MSSP data. Based on this data, researchers built a list of malware families which are currently prevalent and being distributed via attack campaigns.

AgentTesla

Type: Keylogger

Agent Tesla has been distributed by threat actors of all skill levels since 2014. This spyware is a powerful, but extremely easy-to-use password stealing program. Agent Tesla is a credible threat not only because of its advanced functionalities, but because of its availability in underground markets and forums. Agent Tesla is available in a subscription-based manner, where customers pay subscription fees to license the software. These fees range from 11 to 76 USD/10 to 68 EUR depending on features.

GTIC researchers have noticed a 54 percent increase in malicious spam (malspam) campaigns which include Agent Tesla in July. Agent Tesla includes several functionalities for persistence and even has its own custom command and control protocol which uses SSL for encryption. A majority of the malspam campaigns observed include a malicious word document where CVE-2017-11882 (Equation Editor) is exploited and drops a payload which injects .NET code into regasm.exe for further execution.

NanoCore

Type: Remote Access Trojan (RAT)

Although the suspected author of NanoCore was arrested in 2018, GTIC researchers continue to observe almost daily distribution in malspam campaigns. NanoCore is a remote access Trojan (RAT) which was available for sale on hacking forums. Each malspam campaign includes a PDF which leverage jscript, Google Drive and HTML application (HTA) files to install NanoCore. NanoCore has been around since 2013, but based on MSSP data GTIC researchers consider this to be the most popular RAT at the time of this writing. While other RATs such as Remcos, Revenge, and njRAT are still common, campaign numbers are much lower than those of NanoCore. Features include remote control, file manipulations, download-execute, lateral movement and password retrieval. NanoCore is another malware family which relies on injecting .NET code into regasm.exe utility for further execution.

Sodinokibi

Type: Ransomware

Although relatively new, GTIC researchers began observing this ransomware family in May 2019, when the number of infections increased by 23 percent in July alone. Just as Cisco Talos first reported[3], GTIC researchers began observing targeted exploit attempts against Oracle WebLogic vulnerability, CVE-2019-2725[4], followed by the installation of Sodinokibi. This malware family also attempts to exploit a Windows zero-day vulnerability, CVE-2018-8453[5], for privilege escalation. Sodinokibi uses the vssadmin.exe utility to prevent data recovery and deletes shadow copies as well. With no current decryption tool available and intelligence[6] suggesting authors may also be those behind former ransomware king, GandCrab, Sodinokibi is definitely a credible threat.

Revenge

Type: Remote Access Trojan (RAT)

While GTIC researchers have observed more common malware families such as AzoRult, HawkEye, LokiBot, and Formbook in recent weeks, we believe it is important to point out a malware which has not been so commonly talked about, Revenge RAT. In July 2019, GTIC researchers only observed three instances of Revenge RAT, being distributed in typical malspam form. Analysis indicated Revenge has functionality to access webcams, microphones, perform internal recon, spread laterally and of course allow remote control. C2 communication is hidden behind subdomains of blogspot[.]com where malicious content only runs when mshta.exe is used, hiding it from most web debuggers. Revenge has a complex infection chain which differs from most RATs which use malspam for distribution and has redundant C2 infrastructure. Altogether, Revenge RAT may not have as many campaigns distributed monthly, it still poses a significant threat as the tactics, techniques and procedures (TTPs) used differ than traditional RATs and make detection more difficult.

[3] https://blog.talosintelligence.com/2019/04/sodinokibi-ransomware-exploits-weblogic.html
[4] https://nvd.nist.gov/vuln/detail/CVE-2019-2725
[5] https://nvd.nist.gov/vuln/detail/CVE-2018-8453
[6] https://krebsonsecurity.com/2019/07/is-revil-the-new-gandcrab-ransomware/

Sea Turtle: A Tough Shell to Crack

Lead Analyst: Danika Blessman

Earlier this year, researchers published a blog detailing an attack campaign called Sea Turtle[7] – operations at least two years in the making.

Originally identified in April 2019, these operations leverage the domain name system (DNS) – a core piece of the internet – targeting public and private entities, including national security, energy and other mainly government organizations, located primarily in the Middle East and North Africa. In fact, research revealed at least 40 different organizations across 13 different countries which were compromised during this campaign.

As mentioned above, DNS serves as one of the inherently trusted pieces of the internet - corrupting this system calls into question the basic trust model of the internet, causing havoc across the globe as threat actors can redirect a compromised domain to any IP address they choose. While there are several ways threat actors could compromise an organization's – or nation's – DNS records, all methods provide access to manipulate the records, allowing threat actors to modify, add, delete or redirect where an internet user believes they are navigating.

Although most primary target organizations are based in the Middle East, *new* Sea Turtle victims have been spotted in the U.S. and Sudan, including energy companies, think-tanks, and non-governmental organizations.

As these operations are against DNS systems, these attacks have the potential to erode trust and stability of the DNS system – inherent to the basic operation of the internet itself – which could have implications on the global economy or geopolitical climate. Although no attribution to a specific country has been given, technical details of these operations suggest they are being conducted by state-sponsored threat actors, seeking persistent access to sensitive networks and systems.

These are not the first attacks leveraging the DNS system. DNSpionage[8], detailed in November 2018, used the same IP address to redirect legitimate government and private company domains in Lebanon and the United Arab Emirates (UAE). Of note, researchers assess with high confidence that these operations were *not* conducted by the same threat actors as Sea Turtle.

Research showed that there were two clear groups of targets: those which appeared to be the primary target (such as governmental and energy organizations) and those which appeared to be targets in the primary targets' supply chain (i.e.; third party organizations, partners or affiliates of the primary targets through which the primary target could eventually be infiltrated – such as DNS registrars and telecommunication companies).

[7] https://blog.talosintelligence.com/2019/07/sea-turtle-keeps-on-swimming.html
[8] https://blog.talosintelligence.com/2018/11/dnspionage-campaign-targets-middle-east.html

Interestingly, even after technical indicators and details of the group's operations were revealed in April, the group continued operations and actually expanded its target set using similar infrastructure. This is atypical of many state-sponsored groups; after operations, TTPs, and infrastructure are revealed, threat groups often change tactics or the infrastructure from which they operate in order to conceal their activity.

In these campaigns, the threat actors obtain DNS server credentials via phishing or successful vulnerability exploitation. They then modify the DNS records to point users to servers controlled by the threat actors, as in a man-in-the-middle attack. Attackers use this technique to harvest credentials, allowing them additional access to the targeted network – potentially garnering sensitive organizational data.

The blog explained, "In this case, the actor-controlled name server and the hijacked hostnames would both resolve to the same IP address for a short period of time, typically less than 24 hours. In both observed cases, one of the hijacked hostnames would reference an email service and the threat actors would presumably harvest user credentials."

Researchers further noted that one unique feature of this technique which makes the threat actors very difficult to track is that the illicit DNS servers were used ONLY once; each target had its own dedicated name server hostname and IP address. In addition, this technique has been used very cautiously and infrequently.

Researchers recommend several mitigating efforts which organizations can take to minimize the potential threat to this activity, including implementing multi-factor authentication to secure your organization's DNS management, validating all DNS lookups in your recursive resolver, and considering a registry lock service on your domain names.

Indicators of Compromise for the most recent campaigns are available in the blog[9].

[9] https://blog.talosintelligence.com/2019/07/sea-turtle-keeps-on-swimming.html

NTT Security Annual Reports

Risk:Value 2019

In 2019, 33 percent of organizations around the world would consider paying a ransom to a hacker rather than investing more in cybersecurity because paying the ransom is cheaper. Read more about this and other trends in the 2019 Risk:Value report.

Download your copy today!

2019 Global Threat Intelligence Report

This year's report focuses on several security challenges we have observed in organizations over the past year. Our analysis shows an escalation in coin mining, web-based attacks and credential theft, along with changes in the sectors most targeted.

Download your copy today!

Global Threat Intelligence Center (GTIC)

The NTT Security Global Threat Intelligence Center protects, informs and educates NTT Security clients through the following activities:

- Threat research
- Vulnerability research
- Detective technologies development
- Threat intelligence management
- Communication to NTT Group clients

The GTIC goes above and beyond the traditional pure research organization, by taking its threat and vulnerability research and combining it with its detective technologies development to produce applied threat intelligence. Its mission is to protect and provide NTT Security clients with services and tools to prevent and provide early warning notifications of risks and threats 24/7.

Threat intelligence management is where it all comes together. The GTIC continuously monitors the global threat landscape for new and emerging threats using NTT's global internet infrastructure, clouds, and datacenters along with third-party intelligence feeds. NTT Security works to understand, analyze, curate, and enrich threat data using advanced analysis techniques and proprietary tools, then curates and publishes these for the benefit of NTT Security clients using the Global Threat Intelligence Platform (GTIP).

About NTT Security

NTT Security is the specialized security company and the center of excellence in security for NTT Group. With embedded security we enable NTT Group companies to deliver resilient business solutions for clients' digital transformation needs. NTT Security has 10 SOCs, seven R&D centers, over 1,500 security experts and handles hundreds of thousands of security incidents annually across six continents.

NTT Security ensures that resources are used effectively by delivering the right mix of Managed Security Services, Security Consulting Services and Security Technology for NTT Group companies – making best use of local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest ICT companies in the world. Visit nttsecurity.com to learn more about NTT Security or visit www.ntt.co.jp/index_e.html to learn more about NTT Group.