GTIC Monthly Threat Report

November 2019

Contents

NTT Ltd. Monthly Observations 3
Analyzing Attack Categories 3
Vulnerabilities 4

The Evolution of Brute Force Password Attacks 6

We need to talk about Control 8

NTT Ltd. Annual Reports 10
Risk:Value 2019 10
2019 Global Threat Intelligence Report 10

Global Threat Intelligence Center (GTIC) 11

NTT Ltd. Monthly Observations

Lead Analyst: Terrance DeJesus, Threat Research Analyst, Global Threat Intelligence Center

As the holidays approach, NTT Ltd. GTIC researchers analysed MSS data from retail-specific clients, shedding light on more popular cyberattacks targeting the industry – and its consumers – during the holidays.

Analyzing Attack Categories

Analysis of attack categories and subcategories determined brute force and web application attacks accounted for over 72% of all attack categories as shown in **Figure 1**. Based on protocol analysis, adversaries focused on SMB, SSH, and HTTP/S activity targeting SMB accounted for over 90% of all activity. Brute-forcing SMB is nothing new; quite common, in fact, where adversaries leverage tools such as Hydra, Ncrack or Metasploit to attempt a dictionary-based attack.

Although web application attacks were the second largest attack category, analysis indicates activity consisted primarily of blind SQL injection attempts and generic cross-site scripting (XSS) detections.

Category	Percentage
Brute Forcing	50%
Web Application Attack	22%
Malware	21%
Suspicious	3%
Privileged Activity	2%
OS Specific Exploit	2%
All Others	<1%

Figure 1. Attack Categories

According to NTT Ltd. malware detections, over 80% of malware was an information stealer/key logger variant. The most popular malware family being distributed was Agent Tesla, extremely common in malware spam (malspam) campaigns from attackers in Western Africa. Agent Tesla can be bought or rented and comes with robust features which make reverse engineering difficult. As far as retail organizations are concerned,

keyloggers and/or information stealers are bad business as they allow adversaries to steal private information such as store website login credentials. Please note, Agent Tesla is typically found as a portable executable (PE) for Windows computers and not for mobile devices, prompting adversaries to focus their efforts targeting retail client environments.

In addition to this, researchers discovered a surprising amount of activity associated with Vidar malware – an information stealer – in retail network environments earlier this year being distributed via the Fallout exploit kit. The existence of Vidar suggests the possible presence of the Gandcrab ransomware, as the two are often seen in combination. Therefore, not only is private information possibly being stolen but the combination increases the chance of disrupting daily operations if backups are not readily available.

Malware Family	Variant	Percentage
Agent Tesla	Keylogger	28%
Lokibot	Information Stealer	23%
Pony (Fareit)	Keylogger	16%
Vidar	Information Stealer	13%
Hawkeye	Keylogger	6%
Remcos	Remote Access Trojan	5%
Emotet	Banking Trojan/Downloader	4%
Shade	Ransomware	2%
Dridex	Banking Trojan	< 2%
Trickbot	Banking Trojan	< 2%

Figure 2. Malware Detected

Vulnerabilities

As always, it is important to understand which specific vulnerabilities are being targeted as these threats can be mitigated with proper patch management. Regarding retail clients, NTT Ltd. researchers found that adversaries focused heavily on vulnerabilities in Oracle's WebLogic servers. Both vulnerabilities, cited in **Figure 3**, allow for remote

code execution (RCE) if the vulnerabilities are successfully exploited. Even a recent popular vulnerability in vBulletin, CVE-2019-16759, observed a few hits, more than likely focusing on retail forums where customers visit. Rather than targeting customers, though, this vulnerability is likely more commonly used as an entry point before moving laterally in the victim network.

CVE	Company	Hardware/Software	Percentage
CVE-2017-10271	Oracle	weblogic_server	35%
CVE-2019-2725	Oracle	weblogic_server	19%
CVE-2017-5638	Apache	struts	11%
CVE-2015-8562	Joomla	joomla!	11%
CVE-2018-11776	Apache	struts	7%
CVE-2017-14746	Samba	samba	6%
CVE-2018-7600	Drupal	drupal	6%
CVE-2017-12615	Apache	tomcat	2%
CVE-2019-0708	Microsoft	windows_7	2%
CVE-2019-16759	vBulletin	vbulletin	< 2%

Figure 3. Vulnerability-based Attacks

The Evolution of Brute Force Password Attacks

Lead Analyst: Jeremy Bender, Security Intelligence Writer, Threat Intelligence Communications Team, Global Threat Intelligence Center

While everyone may know that they should employ strong, unique passwords, major security lapses still occur from individuals reusing credentials or employing weak and easy to guess passwords. Password reuse puts users, and their associated organizations, at risk of attack from password grabbing malware. In addition, weak passwords increase the likelihood of an attacker being able to compromise an account through brute force attacks, which are currently on the rise.

Between August and October 2019, NTT Ltd. observed a monthly increase in the number of clients impacted by brute force attacks. During the same time period, NTT Ltd. found approximately two-thirds of detected malware had password grabbing functionality. Of this malware, Emotet was the most popular (56% of detections) followed by Agent Tesla (25% of detections).

Similarly, US-CERT, the Department of Homeland Security, and other U.S. federal agencies warned in 2019 about a rise in password spraying attacks which took advantage of users' lax password standards. With this in mind, it is for good reason attackers are interested in passwords and likely view them as an easy way to gain access to an organization.

However, even for users who employ strong passwords, there is still the compounded risk of password reuse and credential breaches. When a password is reused, its effectiveness is questionable. The risk of password reuse is further heightened by the likelihood of password fatigue.

According to LastPass's 2019 Global Password Security Report[1], the average employee at a large organization (that is, over 1,000 employees) needs to memorize up to 25 unique logins. For employees of smaller companies, the average number of unique logins rises to 85. This inevitably leads to some employees reusing passwords, employing easy to remember – and thus easy to predict – variations of a base password, or using passwords which are easy to crack in dictionary attacks.

The risk of dictionary and brute force attacks increases further if the attacker can gather information about the user via social media – potentially increasing the chances they can identify an interest the user may include in their common passwords. This problem is compounded with the potential use of AI-enhanced brute forcing tools. Such enhanced tools could use an individual's publicly available social media data to better predict a target's password by linking the target's interests to potential phrases. Such tools could also use previously leaked data about a target to better construct what their passwords may be. Due to this, the enhanced tools can more accurately and quickly guess a password instead of having to work through every potential variation.

[1] https://www.lastpass.com/state-of-the-password/global-password-security-report-2019

It is likely AI-enhanced brute forcing tools will proliferate or be used in tandem with current password guessing tools. Current tools, such as Hashcat and John the Ripper, are already highly effective at cracking passwords and password recovery. Hashcat, for instance, can produce hundreds of millions of passwords based on human-created rules. However, there is a ceiling to the number of passwords these programs can guess, and the programs require years of manual coding and improvements to attain this level of precision.

The danger AI and machine learning-enhanced brute force tools pose, as compared to programs like Hashcat, is their ability to improve and change as they function. For instance, in 2017, researchers at Stevens Institute of Technology created a deep-learning generative adversarial network (GAN) called PassGAN.

In a direct trial, PassGAN did not generate as many correct passwords as Hashcat. However, unlike Hashcat, PassGAN could create its own password creation rules as it functions. This allows PassGAN to guess passwords indefinitely. Additionally, PassGAN can become more functional as additional neural network layers are added to it and as it is trained on more leaked passwords. The highest number of correctly generated passwords, however, was created through a combination of PassGAN and Hashcat. This illustrates how attackers could also make current tools more effective without having to create brand new tools of their own.

Also, in 2017, a research team at Carnegie Mellon trained[2] a neural network so it outperformed other password guessing models – such as Markov predictive models and Hashcat. The neural network generally became more accurate as its model size increased. Based on this, brute force tools employing neural networks and large credential breach inputs could become more common and effective at password cracking.

Fortunately, even if brute force tools do continue to improve and become more effective, mitigations continue to exist. Users can shield themselves from brute force attacks by employing simple measures such as using strong, unique passwords for every login. Users can also avoid password fatigue by employing password managers. Beyond staff policies and training - to include user awareness and policies, along with technical controls – organizations can limit the efficacy of brute force attacks by employing multi-factor authentication and by limiting the number of incorrect login attempts before temporarily locking an account.

[2] https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/melicher

We need to talk about Control

Lead Analyst: Dom Newton, Senior Manager, Global Privacy and Data Protection

No, this is not another retrospective on the all-too-brief life and music of the Joy Division front man. A few days spent with privacy peers at the International Association of Privacy Professionals (IAPP) Brussels[3] detailed the hottest – and by the far the most opaque to many – topic: the growing body of caselaw relating to the topic of data controller; more specifically – when you are *joint* data controllers.

This may seem a bit of an arcane concept (because it is) which should only concern the appointed privacy geek in the business. However, the implications of having a closer, though possibly less well-defined relationship, with your 'partners'/'vendors'/ 'stakeholders'/'significant other' than you had previously thought, goes well beyond the dry text within your data processing agreements and which version of the European Union (EU) model clauses your legal team copy and paste into your schedules.

Heading briefly back to first principles, the concept of data controller in EU law is supposed to provide the individual whose data is being processed with clarity as well as a point of contact by which they can exert their data rights. The controller, under both the old EU 1995 Data Directive and the new General Data Protection Regulation (GDPR), is the party who decides the (hopefully lawful) purposes of the processing and the means by which it takes place. This is distinct from the 'processor' who, although still liable for infractions, is effectively an agent of the Controller and must follow their instructions.

So far, so good? Well, as incumbent privacy geek, it's not always that simple. Where a processor has a degree of autonomy, does that cross the line into *de facto* Controller status? If so, are there a ton of responsibilities which follow? And then, to what extent is control of that data shared with the other Controller? Are they, in GDPR language, 'joint controllers'?

Recent cases have led to a major reappraisal of this – the extent to which jointly defining purposes, via placement of a 'Like' button, or a shared aim such as proselytising a particular viewpoint – even while you do not have access to the data being processed, or cannot exert meaningful influence on the actual processing activity. This has rapidly expanded in cases in Germany and elsewhere. You will be accountable for any processing which you may cause to happen or in which you have a shared, common interest.

The effect of this will need to be a review of all but the most basic of relationships – and, reluctantly, a significant addition to those ever-growing Data Processing appendices.

The other element to all of this is that there will be side effects into more practical parts of data protection compliance. Looking specifically at security, for instance – in

[3] https://iapp.org/conference/iapp-europe-data-protection-congress/

technical and organizational measures (TOMs), we will be moving away from a position where the Controller can, in most cases, dictate the security terms to its processor via the TOMs. Liability usually follows, to a greater or lesser extent, depending on the parity of the parties.

However, in a joint controller relationship, responsibility (and thereby liability) is much less cleanly defined. Although you need an Article 26 agreement to define the relationship and roles in respect of rights, etc., the sting in the tail is that the individual can still go for either or both the Controllers in the event that something goes wrong, or to exercise their rights – as, of course, can the regulator.

So, we move from the position where TOMs are something handed down, to something which has to be much more closely reviewed – and perhaps even jointly managed – and where elements such as third-parties take on a whole new meaning.In a Joint Controller relationship, does the Joint Controller's third-party in effect become your own, and how can you exercise control?

From the service provider perspective, how do you contact data subjects to inform them that you are suddenly a data controller, when they have never heard of you, and doing so may breach confidentiality arrangements – and how do you handle the exertion of their rights? From the service provider perspective, how do you contact data subjects to inform them that you are suddenly a data controller, when they have never heard of you, and doing so may breach confidentiality arrangements – and how do you handle their exertion of their rights? Do you refuse business on the grounds that a *customer's* security posture does not offer adequate safeguards?

We wait, with bated breath, the European Data Protection Board's updated guidance in this area – but from conversation in the last few days, the regulators seem as stumped as most commentators by how to practically approach this issue.

In the meantime, effective compliance arrangements, supplier controls, and security controls will take on ever greater importance – choosing the right trusted partner may be critical as the relationship is forced (by the courts and regulators) to be far closer than either party may have wished or understood…

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

- Threat research
- Vulnerability research
- Detective technologies development
- Threat intelligence management
- Communication to NTT Ltd. 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 Ltd. 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 Ltd.'s global internet infrastructure, clouds, and datacenters along with third-party intelligence feeds. NTT Ltd. works to understand, analyse, curate, and enrich threat data using advanced analysis techniques and proprietary tools, then curates and publishes these for the benefit of NTT Ltd. clients using the Global Threat Intelligence Platform (GTIP).

About Security and NTT Ltd.

Security is a division of NTT Ltd., a global technology services company bringing together the expertise of leaders in the field, including NTT Communications, Dimension Data, and NTT Security. The Security division helps clients create a digital business that is secure by design. With unsurpassed threat intelligence, we help you to predict, detect, and respond to cyberthreats, while supporting business innovation and managing risk. Security has 10 SOCs, seven R&D centers, over 2,000 security experts and handles hundreds of thousands of security incidents annually across six continents. Security ensures that resources are used effectively by delivering the right mix of Managed Security Services, Security Consulting Services and Security Technology.

NTT Ltd. partners with organizations around the world to shape and achieve outcomes through intelligent technology solutions. For us, intelligent means data driven, connected, digital, and secure. As a global ICT provider, we employ more than 40,000 people in a diverse and dynamic workplace, and deliver services in over 200 countries and regions. Together we enable the connected future. Visit us at our new website hello.global.ntt