GTIC Monthly Threat Report

October 2019

Contents

Monthly Observations Section

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

During the month of October, the Global Threat Intelligence Center (GTIC) analysed vulnerability-specific activity within current, global, GMSSP data.

Based on volume alone, the most targeted application was Apache Struts, accounting for 78% of all application-specific activity. Apache Struts – particularly CVE-2017-5638 – is continuously targeted by internet-wide scanning by botnets. This serves as yet another reminder that older vulnerabilities continue to be targeted, and users should patch their systems.

Generally, the most common vulnerabilities targeted in internet-wide scanning or opportunistic attacks allow remote code execution and are relatively simple to execute. Proof-of-Concepts (PoC) are readily available and compiled code in large botnets are capable of generating HTTP payloads which can exploit these vulnerabilities. **Figure 1** shows some of the most highly targeted software over the past month. All of these technologies have similar vulnerabilities in specific versions that are just as easily exploitable. High attack volumes can indicate a highly targeted attack, but in many cases, high volume can be considered noise and not pose the same risk as a more targeted attack. Active patch management should always be regarded as a top priority for these systems as newer vulnerabilities for the same software are likely.

Software	Company	# of Vulns Targeted in October	Percentage of All Vuln Activity
Struts	Apache	9	78%
Tomcat	Apache	1	2.4%
WebLogic Server	Oracle	3	< 1%
Office	Microsoft	2	< 1%
JDK	Oracle	1	< 1%
Joomla!	Joomla!	2	< 1%

Figure 1: Top 5 software vulnerability activity

GTIC researchers also compared the most recently disclosed vulnerabilities with attacks observed in the wild. Given its recent discovery, it is not surprising that vBulletin vulnerability CVE-2019-16759 is listed as number one. CVE-2019-16759 is a remote code execution vulnerability in the popular content management system vBulletin, and a PoC was made available within hours of disclosure. NTT Ltd. observed industries targeted by this vulnerability include technology, health care, retail, finance, and

government. Attacks against technology and health care accounted for more than 90% of this activity. Further analysis showed attempts to implement a PHP-based backdoor on vulnerable systems.

Date disclosed	CVE number	Affected Vendor	Affected software
24 Sept 2019	CVE-2019-16759	vBulletin	vbulletin
09 Aug 2019	CVE-2019-14234	Django project	django
19 June 2019	CVE-2019-2729	Oracle	weblogic_server
26 April 2019	CVE-2019-2725	Oracle	weblogic_server
21 Feb 2019	CVE-2019-6340	Drupal	drupal

Figure 2: Targeted vulnerabilities prioritized by most recent disclose date and activity volume

GTIC found that 81% of all vulnerability-based activity in October allowed remote or arbitrary code execution if successfully exploited. Coupled with relentless botnet distribution, unpatched systems are more likely to be compromised. NTT Ltd. Limited recommends prioritizing patch management for critical system components to best mitigate risk. While more targeted attacks will leverage various tactics, techniques and procedures (TTPs) which involve less critical vulnerabilities, business or network operations could be severely disrupted from opportunistic-focused adversaries.

Drone Security– Risks and Rewards

Lead Analyst: John South, Senior Director, Global Threat Intelligence

Drones, or Unmanned Aerial Vehicles (UAVs), are becoming more common for recreational, commercial, and academic users. Commercial uses include physical site and plant inspections, windfarm maintenance, precise delivery of chemical applications to alleviate crop disease, real estate photography, natural disaster response, and development of highly accurate maps. Academic uses include surveys of archaeological sites, measuring air pollutants, hydrology studies including storm surge evaluations before natural disasters, and research on the health of forests. Sometime during or after the flight data is downloaded to a corporate, academic, or personal network.

Many UAVs today use a spread spectrum technology to switch between one of 23 channels every 11 milliseconds to avoid conflict with other aircraft. Jonathan Andersson demonstrated his ICARUS[1] device at the PacSec Conference in 2016. ICARUS harvested the shared secret and then took remote control of the aircraft[2]. The attacker gets physical control of the drone and all data it contains.

Restricted airspace is another drone-related issue. The Heathrow and Gatwick airports use a Drone Dome system to counter unauthorized UAVs. The system can detect and identify a UAV, and it can also use a short burst of microwaves to destroy the aircraft. This is only one of many available anti-drone solutions.

The Tactical High-Power Microwave Operational Responder (THOR) was developed by the United States Air Force Research Laboratory to use short bursts of high-powered microwave signals to knock down short range UAVs which have been identified in unauthorized flight paths. For longer range swarms of UAVs, the Air Force will use the Counter-Electronic High-Power Microwave Extended-Range Airbase Air Defense system (CHIMERA) when it becomes available in 2020.

Concern Over Foreign Manufactured UAVs

Industry has expressed concern about foreign-produced aircraft transferring data back to their manufacturers. The U.S. Department of Homeland Security (DHS) issued an alert[3] that some UAVs "contain components which can compromise your data and share your information on a server accessed beyond the company itself." One risk is that private information – data, including video, location, time, or flight parameters – may be passed on. A bigger concern is that data on servers may be accessed while the UAV is connected for software updates or data downloads.

[1] https://www.digitaltrends.com/cool-tech/trend-micro-icarus-drone-hijacking/

[2] https://www.youtube.com/watch?v=S6MER2mvjUw&feature=youtu.be

[3] https://edition.cnn.com/2019/05/20/politics/dhs-chinese-drone-warning/index.html

DJI (who holds the largest market share of UAV sales at 76%[4]), stated that they provide UAVs for government and critical infrastructure[5] use which "…do not transfer data to DJI or via the internet, and our customers can enable all the precautions DHS recommends."

In September, the U.S. Senate began discussing a bill to prohibit the procurement of off-the-shelf drones or any subcomponents from specified foreign entities (and subsidiaries or affiliates) which pose a national security risk.

Goldman Sachs estimates the current market for UAV-based job opportunities is worth about USD 23.2 billion[6]. Businesses are looking to UAVs to help with tasks which have historically been more expensive, or even more dangerous, to accomplish via conventional means. In the end, there are risks with UAVs, but, in many cases, their value has outpaced the risks.

Recommendations

- Responsible organizations and individual pilots must validate all flights are following proper regulations. Pilots are responsible for ensuring they comply with all appropriate local laws and obey all property rights for any lands they fly over.
- As part of their pre-flight checks, pilots must ensure software is up-to-date in all UAV flight systems, such as the flight controller, peripheral equipment, batteries, and the differential global positioning system.
- The organization or pilot must ensure the flight privacy mode is enabled on aircraft which have that capability installed. This prevents any flight data and images from being sent back to the manufacturer.
- Hacking UAVs has become a reality within the last few years. However, as most flights are in the local area, the risk of hacking the aircraft flight controller is limited. As more companies become certified to fly Beyond Visual Line of Sight (BVLOS), it may be important to think about this risk.

It is important to understand the responsibilities imposed upon UAV pilots. The pilot is the individual responsible for all aspects of any given flight. Errors in judgement, skill, or faulty equipment can lead to damage of the UAV, the infrastructure site, or worse.

[4] https://dronelife.com/2019/10/01/droneii-dji-is-number-1-check-out-number-2-and-will-the-proposed-drone-security-act-change-anything/

[5] https://www.businessinsider.com/us-government-warns-drones-from-china-pose-spying-risk-report-2019-5

[6] https://www.goldmansachs.com/insights/technology-driving-innovation/drones/

The DevSecOps Approach for Driving Better Outcomes

Lead Analyst: Kashif Hafeez, Senior Director, Product Marketing, WhiteHat Security

Applications have become one of today's most critical business drivers. Consequently, application security-related risks are one of the most significant business risks. With technological advances comes the promise of increased efficiency and performance for business applications. At the same time, inadequate and ill-designed application security approaches expose organizations to risks. This is according to our latest Application Security Statistics Report[7], a comprehensive analysis on what's working, and what's not, in the world of application security.

The good news is organizations are more aware than ever of their application security risks, with a 20% increase in the number of applications being tested.

The bad news is remediation rates have fallen. The remediation rate for critical risks, for example, is 50.7% in the U.S. and just 40.7% in Europe.

Also hampering organizations' ability to keep up with vulnerabilities are the embeddable components in the software supply chain, which account for one-third of all application vulnerabilities. In fact, WhiteHat Security found a 50% increase in unpatched library vulnerabilities this year. This is a dangerous trend, as more open-source and third-party software is embedded in organizations' own applications. It also underlines the need for software vendors to raise their security standards.

It is clear organizations should make DevSecOps an integral part of their application development and delivery strategy. This means embedding security in their development and operations in a phased approach – one which offers a clear roadmap for comprehensively addressing the diverging needs of existing in-production applications and an increasing number of new applications.

In the Application Security Statistics Report, WhiteHat Security identifies three metrics-driven phases which are proven to succeed in securing applications.

Phase 1 – Risk Discovery and Management: Key Metrics

Window of Exposure – this metric represents the amount of time an application has a serious vulnerability which can be exploited and lead to data breaches. As such, organizations should develop a service level agreement (SLA) for "Window of Exposure" and aggressively try to reduce it for all their applications.

Time-to-Fix by Risk – this is a baseline for how long it takes to fix a vulnerability and associates that with risk. Developing an SLA for "Time-to-Fix by Risk" and working aggressively to reduce it for vulnerabilities in applications is, critical.

Remediation Rate by Risk – this represents the percentage of vulnerabilities which are fixed, organized by level of risk. Develop SLAs and procedures/training to promote

[7] https://info.whitehatsec.com/Content-2019-StatsReport_LP.html

remediation by taking a risk-based approach. Track metrics to ensure the most serious vulnerabilities are being prioritized for remediation.

Phase 2 – Release Assurance: Key Metrics

Average Time-to-Fix (SAST) – this metric provides an industry baseline for how long it takes to fix a vulnerability in general. Organizations should develop an SLA for this metric and aggressively try to reduce it for all vulnerabilities.

Remediation Rate by Risk – this represents the percentage of vulnerabilities which are fixed, organized by level of risk. Develop SLAs with procedures and training which promote remediation efforts by taking a risk-based approach. Track the "Remediation Rate by Risk" metrics to ensure the most serious vulnerabilities are being prioritized for remediation.

Vulnerability Prevalence by Class (SAST) – in order to rapidly innovate, organizations are increasingly adopting open source and commercial off-the-shelf components. As such, the likelihood of inheriting vulnerabilities is higher than before. Baseline development teams' security goals by creating an SLA around reducing the most likely vulnerabilities by class.

Phase 3 – Developer Enablement: Key Metrics

Vulnerability Prevalence by Class (DAST and SAST) – use this to set up focused and recurring training for development, operations, and security teams. Track teams' progress by tracking Vulnerability Prevalence by Class for the applications they develop and evolve training efforts to meet each team's evolving needs.

DAST and SAST Remediation by Risk – use the "DAST and SAST Remediation by Risk" metric to baseline teams' goals. Develop SLAs and procedures/trainings which promote remediation efforts by taking a risk-based approach. Track the "DAST and SAST Remediation by Risk" metrics to see that the most serious vulnerabilities are being prioritized for remediation.

About WhiteHat Security

WhiteHat Security is a wholly-owned, independent subsidiary of NTT Ltd.. With this strategic development, we are able to combine the global reach of NTT Ltd. with WhiteHat's deep expertise in application security. As a result, our research offers the most comprehensive perspective on the current state of application security, as well as recommendations on how to implement DevSecOps effectively.

Disinformation-as-a-Service: Now Targeting Private Corporations

Lead Analyst: Danika Blessman, Sr. Threat Intelligence Analyst, GTIC

Disinformation operations are typically thought of in a "spy-versus-spy" manner – as tools of espionage by rival (or even friendly) governments. More recently, such disinformation activities have been in the news as governments continue to leverage social media and other internet outlets to influence public opinion and the outcomes of elections.

With so much of the attention focused on nation-state-sponsored disinformation campaigns, it's easy to overlook all of the other potential applications of Disinformation-as-a-Service (DaaS).

Some of this activity is quite impactful, and, fortunately, continues to be dismantled by social media platforms; Facebook and Twitter have successfully removed hundreds, thousands, and in some cases, hundreds of thousands of fake accounts associated with bots or nation-state-backed campaigns

This is a global problem, affecting countless political and social issues worldwide – allegations of Russian exerting influence in everything from Brexit to elections in Belgium, France, and the U.S. continue to gather attention. These practices are extending to targeted advertising, effectively influencing everyone with an online presence.

Along with any political ramifications, potentially billions of dollars are at stake for advertisers, consumers, organizations or nation-states. It's no wonder that disinformation campaigns – via social media, news outlets and other platforms – have become so successful. So much so, in fact, that cyber criminals are now following in these footsteps, providing DaaS for as little as a few hundred U.S. dollars in underground forums, available for anyone to purchase. Rather, though, than attempting to influence public opinion or elections, these campaigns are being leveraged in the private sector as the newest tool for corporate espionage.

New research[8] by Recorded Future's Insikt Group shows it is "alarmingly simple and inexpensive" to launch a sophisticated disinformation campaign.

DaaS enables corporations — via highly customizable offerings — to generate not only positive publicity for themselves but also negative media for competitors. This is achieved by both exploiting social media and by having cyber criminals create an entire media campaign — including news articles and blogs — to promote the hiring organization's agenda.

[8] https://go.recordedfuture.com/hubfs/reports/cta-2019-0930.pdf

The ideas behind DaaS — disinformation, propaganda, smoke screens, false flags, and perception management operations — are not new, but they have become the "new normal." In fact, according to the Oxford Internet Institute[9], this "new normal" includes both toxic messaging spread on a global scale and tools leveraged for targeting – and amplifying – this disinformation.

DaaS campaigns against an organization could ultimately have immeasurable consequences, including substantial financial risk — such as stock price manipulation or affecting your organization's bottom line — as well as severe reputational damage.

Again, these tactics are not new, but the tide is turning to include operations against those outside of the traditional spy-versus-spy campaigns — targeting citizenry, corporations, individuals, and even veterans' groups. The greatest challenge may be that these threats continue to evolve technologically and proliferate. And, given how easily and inexpensively DaaS can be acquired, it is likely the risk will only become more significant to private corporations.

So, what can you do to prevent or protect your organization?

Organizations need to be incredibly focused on any erroneous information published in news sources, social media, or other digital or printed resources. This can be accomplished using a brand-monitoring solution which can alert any mention of your brand.

Organizations should also consider a counter-disinformation campaign in the event they are targeted. Create positive brand content and distribute as widely as possible — and use search engine optimization to promote this positive brand content.

Legal action may also have to be a possible recourse.

Solutions to this growing issue will likely rely on a combination of government, news media, corporation and individual actions and support. Ultimately, though, corporations need to be the most heavily involved in their own brand protection and security.

[9] https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf

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!

NTT Ltd. In the Spotlight

Congratulations to Edith Santos, Director of Global Incident Response for NTT Ltd., who was named a Cyber Defense Magazine Global Award Winner for 2019 in the Women in Cybersecurity category. Read more at the Cyber Defense Global Awards 2019[10] site.

[10] https://cyberdefenseawards.com/cyber-defense-global-awards-winners-for-2019/

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