NTT Security

# GTIC Monthly Threat Report

June 2019

A Global Threat Intelligence Center
publication from NTT Security

# Contents

# GDPR: A Year In, and the Regulators are Starting to Bite

**Lead Analyst: Dominic Newton**

We're now over a year into the world of GDPR and are finally starting to see the shape of enforcement from regulators. We are also awaiting answers on some of the biggest questions - the future, courtesy of the 'Shrems II [1]' case, which will assess the legal validity of the current EU Standard Contractual Clauses cross-border data transfer mechanism; the review of the EU/U.S. Privacy Shield data transfer mechanism (now pushed out until the Court of Justice rules on Shrems II); and, for anyone touching the UK or Brexit.

On enforcement, the Commission Nationale de l'Informatique et des Libertés (CNIL) decision to fine Google €50m (subject to appeal) is a definite outlier, and one, at that, which has caused no small confusion. Regulatory guidance is generally to layer Privacy Notices to help make them more accessible – so the reader does not need to scroll through reams of legalese, but can navigate cleanly to the bit they're interested in. However, the CNIL enforcement decision then seems to be based on the number of clicks by an end-user to get to the part of the notice they wanted to – the more clicks, the worse, encouraging exactly the kind of flat but inaccessible notices of pre-GDPR days.

Adding further to the confusion around privacy notices and consent is the deep regulatory and legislative concerns on the AdTech industry and its impact on individual privacy. Far from just a GDPR issue, it has resulted in cookie requirements – an increasingly hazardous area to try to gain GDPR-level consent, especially when selling ad space. And, the U.S. has driven the California Consumer Privacy Act (CCPA), firing the starting gun on a plethora of other U.S. state-level privacy laws and dusting off the idea of a U.S. federal law. As GDPR trundles on, business as usual, for those touching California data, CCPA is likely to consume a similar amount of resources– and elicit a similar amount of anxiety – as we approach the end of 2019.

But what about other GDPR enforcement? Where have the largest fines hit so far? It may be an interesting statistic that of the €56m fines levied so far, €50m comes from the Google case alone. Some

[1] https://www.techdirt.com/articles/20190118/16302241424/max-schrems-files-new-privacy-complaints-that-seem-to-show-impossibility-complying-with-gdpr.shtml

of the caution in other regulators not going for larger fines may be derived from the European Data Protection Board's edict that individual regulators should harmonise their approach.

The other large-fine cases are an interestingly mixed group – and most are not, at the moment, old-fashioned breaches (at time of writing, regulatory action has not yet been announced on two high-profile cases). Instead, the regulators have, so far at least, been far more concerned about snooping, excessive retention and security controls.

So, this is the real lesson – getting breached isn't what gets you fined; it's the evidence of poor compliance and controls that the regulator finds which gets you over the line into enforcement territory.

NTT Security top recommendations are:

- **Make sure you have Data Protection designed into your business change processes** – this means bringing in the privacy and security teams at the *start* of any change programme, not asking them to bolt on compliance at the end, and letting them appropriately challenge use of data so the business fully understands – and can demonstrate – *why* it is using personal data in that way. Data Protection must be treated like a basic business requirement.
- **Get your Privacy Notices in good order and keep them up-to-date** – and your cookie notices too. If you're relying on consent, especially for marketing, make sure you can tie individual consents to records, and that you can show *what* was consented to.
- **Get rid of data you don't need** – good housekeeping is key; if you don't have it, it can't be hacked and isn't a risk to the rights of individuals. Make sure your operational teams know what the laws are surrounding data retention and get both policy and processes in place to enforce them.
- **Security is still key** – invest in appropriate security; although most organizations can expect to be breached, failure to put basic security controls in place will get you fined – and open up the rest of your processing operations to inspection. You should also test your breach response capability regularly – the manner in which a breach is handled often makes a huge difference both to any reputational damage, and how the regulator view it – so, test, test, test!

# Where BlueKeep is Now?

**Lead Analyst: Jon Heimerl**

## What is BlueKeep?

As of mid-June, 2019 has seen over 5,400 new vulnerabilities. CVE-2019-0708, first defined in May, is only one of those vulnerabilities, but it is not "just another vulnerability."

CVE-2019-0708, dubbed BlueKeep, is a remote code execution vulnerability in Microsoft Remote Desktop Services[2] (RDP - formerly known as Terminal Services). If an attacker connects to the targeted system using RDP and sends a specifically crafted request, they could execute arbitrary code on the victim system. Successful exploitation would allow an attacker to install programs, access data, or create new accounts with full user rights.

The vulnerability is exposed pre-authentication – so not only does the attack work remotely, but an attacker does not need to be authenticated to access the targeted device. The vulnerability could also potentially be exploited by self-propagating worms, increasing the danger of rapid spread from vulnerable system to vulnerable system through automated attacks – no credentials or user interaction required.

The vulnerability affects Windows versions 2000 through 2008, including Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2. So, while BlueKeep does not affect Microsoft's more current operating systems like Windows 8, Windows 8.1, Window Server versions 2012 and later, or Windows 10, that still means there are potentially millions of vulnerable systems that may be targeted.

## Is BlueKeep Real?

Before the end of May, researchers began demonstrating proof of concept (PoC) attacks against BlueKeep. On 5 June, a security researcher revealed that he had created a Metasploit module which exploited the BlueKeep vulnerability on some systems.

[2] https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

PoC code appeared on several GitHub websites. Many researchers were hesitant to release PoC code publicly, though, as the vulnerability could have led to a wormable RDP malware attack. Despite this, the patch released by Microsoft was reverse-engineered to create a workable PoC, released days later on GitHub.

GTIC researcher, Terrance DeJesus, observed NTT Managed Security Services data almost immediately revealed a 52 percent increase in port 3389 (the port used by RDP) traffic, however, none specifically targeted CVE-2019-0708 until June. During May, researchers observed active probing against mainly education, manufacturing, technology, and finance clients. Most of this probing was from servers hosted in the U.S., other locations such as Germany, Canada, Netherlands, United Kingdom, France, and Liberia were also observed. No specific commands were observed being sent to targeted hosts, rather the third-layer of the RDP connection sequence (Client -> MCS connect-initial -> Server) was observed before sessions were closed after a response was given. While some of this activity originated from sites associated with various researchers, other sites included a history of nefarious activity.

## Is BlueKeep a Big Deal?

BlueKeep quickly drew comparisons to WannaCry – a wormable vulnerability potentially affecting as many as a million systems. The “good news,” if there was any, was that there were no known exploits at the time the vulnerability was released, but that changed quickly.

Microsoft has issued multiple advisories on BlueKeep. On 14 May, Microsoft issued an advisory specifically for CVE-2019-0708, in which they labelled the vulnerability with a CVSS of 9.8 and advised users to patch immediately. At this time, Microsoft released patches to address the vulnerability, including for versions of Windows which were considered “out-of-support”. Microsoft issued a second advisory on 30 May, urging users to apply available patches.

In general, the security industry recommended users patch and take mitigating actions to remedy the vulnerability. But on 4 June, the United States National Security Agency (NSA) released an advisory[3] urging organizations and Windows administrators to take BlueKeep seriously and to ensure they are patching and taking other appropriate actions to protect themselves. This was only the NSA’s third such advisory in 2019.

[3] https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csa-bluekeep_20190604.pdf?ver=2019-06-04-123329-617

On 17 June, the United States Cybersecurity and Infrastructure Security Agency, as part of the Department of Homeland Security issued Alert[4] (AA19-168A) advising users and administrators to review the available Microsoft information, patching and applying mitigation actions "as soon as possible."

Microsoft, the NSA, CISA, and others re-iterated the fact that BlueKeep has the potential to become a WannaCry or Petya-level problem, if organizations do not take action to mitigate the vulnerability immediately.

## What do I Really Need to Do About BlueKeep?

First of all, take it seriously. BlueKeep has the potential to be a big deal for organizations with affected systems. By all accounts, that is likely *millions* of systems.

Secondly, you need to take action:

1. **Patch.** Patch your affected Microsoft operating systems per Microsoft guidance[5].
2. **Disable Remote Desktop Services.** Removing unnecessary services is good security practice in general, and can help make your environment less vulnerable.
3. **Block port TCP 3389.** Since RDP uses port 3389, blocking this port can effectively stop communications and exploit attempts.
4. **Upgrade.** Consider upgrading to fully supported Microsoft operating systems which are not affected by BlueKeep.

[4] https://www.us-cert.gov/ncas/alerts/AA19-168A

[5] https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708

# Linux Systems Stung by "HiddenWasp"

**Lead Analyst: Danika Blessman**

Researchers have identified a new type of malware targeting Linux systems. The malware, called HiddenWasp[6], appears to be used as part of a second-stage attack against already-compromised systems. It is an advanced backdoor attack tool which allows complete remote control of the targeted system.

Originally uploaded to VirusTotal by Shen Zhou Wang Yun Information Technology Company, a China-based forensics firm, researchers identified the malicious files on VirusTotal in April 2019. The role of the forensics company in relation to the malware is unclear.

The malware itself consists of three components: an initial deployment script, a rootkit and a Trojan. The rootkit and Trojan provide persistence in the targeted system and allow full control of the victim host.

While a majority of Linux malware is focused on crypto-mining or distributed denial of service (DDoS) activity – likely for financial gain – HiddenWasp appears to be purely used for remote control of the targeted Linux system or network, suggesting that victims are specifically chosen.

The HiddenWasp Trojan also appears to be leveraged as a second-stage payload; that is, targeted machines were previously compromised by the attackers. The initial infection vector is unknown – or at least not disclosed in the research.

Attribution is also unknown. HiddenWasp – assessed with low confidence to be of Chinese origin since it has similarities to other Chinese malware families – was adopted leveraging a large amount of code from various open-source malware and rootkits such as Mirai and Azazel.

[6] https://www.intezer.com/blog-hiddenwasp-malware-targeting-linux-systems/

Targeted machines were not disclosed in the research; in fact, many are likely unknown. The files discovered on VirusTotal, however, had timestamps dating back to November 2018, suggesting any targets could have become infected at least that long ago – and may still be.

HiddenWasp is also unique because of its evasion properties – in fact, it "has a zero-detection rate in all major anti-virus systems," according to the research. It is important to note, though, that AV software for Linux systems tends to not be as robust as in other platforms.

Frighteningly, HiddenWasp malware is still active in the wild.

Researchers recommend the following mitigation efforts against the HiddenWasp malware:

- Block the command-and-control IP addresses detailed in the indicators of compromise (IOCs) of the report.
- Run the provided YARA rule against in-memory artifacts to detect these implants.

Researchers also recommend checking your system for "ld.so" files — if any of the files do not contain the string '/etc/ld.so.preload', your system may be compromised, as the Trojan implant attempts to patch instances of "ld.so" to enforce the LD_PRELOAD mechanism from arbitrary locations on the system.

# NTT Security Observations: High Risk Vulnerabilities Being Scanned

**Lead Analyst: Terrance DeJesus**

## Exim Mail Transfer Agent (MTA): CVE-2019-10149

In early June, Qualys released a security advisory[7] for a vulnerability discovered during a code review of Exim. The vulnerability could allow remote code execution (RCE) and was exploited by adversaries prior to disclosure. To exploit the vulnerability remotely in a default configuration, an attacker needs only to keep a connection to the vulnerable server open for seven days. The vulnerability exists in the deliver_message() function, allowing an adversary to send mail to the server in which expand_string() is used to run arbitrary commands by default. If combined with @localhost as the address, a local domain is chosen.

As shown in a recent Shodan search[8], almost three million vulnerable public-facing Exim servers exist, a majority of which are hosted in the U.S. GTIC researchers continue to observe active CVE-2019-10149 probing against clients in the Finance industry, where vulnerable hosts are being logged to remote servers as shown in **Figure 1**.

[7] https://www.qualys.com/2019/06/05/cve-2019-10149/return-wizard-rce-exim.txt?_ga=2.86954077.457439207.1561386583-212428892.1561386583

[8] https://maps.shodan.io/#16.720385051693988/3.515625/3/satellite/Exim%204.92

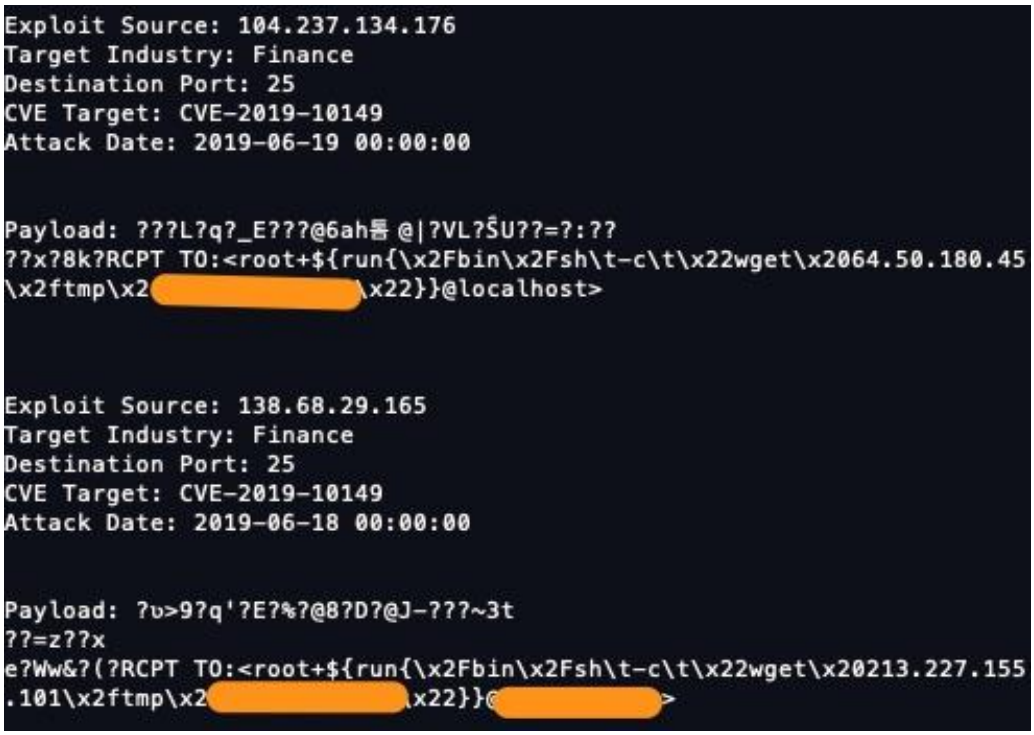


**Figure 1**. Probing against CVE-2019-10149 and logging to remote servers

With the popularity of the Exim MTA, along with the observation of active probing, NTT Security highly recommends patches be applied as soon as possible. NTT Security currently has active detections in place to identify exploit attempts against this vulnerability.

# 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 of the new 2019 Risk:Value 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.