Royalty-free stock illustration ID: 1395082445

Jun 11, 2021 10:47 BST

Research update: RM3 – Curiosities of the wildest banking malware

Recently, our Research and Intelligence Fusion Team (RIFT) published research findings on RM3, an advanced variant of the banking malware family known as Gozi and uncovered Oceania as the top target for threat actor groups.

Gozi variants, which target financial institutions, are operated by a variety of threat actors. Typically, they cause financial losses through direct involvement in transactional fraud, or by facilitating other types of malicious activity such as targeted ransomware activity.

In 2017, the RM3 variant was detected with a number of major modifications compared to the previous main variant, including a rebranded RM loader, an exotic and exclusively designed PE file format, a modular architecture, a reworked network communication and new modules.

Our RIFT identified approximately 136 financial institutions that had been targeted by threat actor groups using RM3 since 2017. Around two thirds of those institutions are based in Oceania, with an estimate of 21% based in the UK and 12.5% based in Italy. More than 90% of the financial institutions that were targeted across those regions are banks, with web shops (<1%), job websites (1%), loan websites (1%) and crypto services (4%) representing some of the other organisations to be targeted.

According to our research from the last 30 months, threat actors are using RM3 in drastically different ways across Oceania and Europe.

In Oceania, we observe that threat actors appear to have significant experience and use traditional means to conduct fraud and theft, mainly using web injects to push fakes or replacers directly into financial websites. It is noteworthy that some of these injectors are more advanced than the usual ones that are usually seen in banking malware, and suggest the operators behind them are more sophisticated and experienced.

In Europe we see different behaviour, where threat actors generally follow a manual fraud strategy.

Christo Butcher, NCC Group's Global Business Unit Head for Threat Intelligence comments: "Over the years, we've seen the disruption that well-crafted malware can cause – particularly in highly-targeted industries such as the financial sector. RM3 is a very sophisticated variant, with threat actors targeting organisations around the world using tailored methods, so it's important that banks and other financial businesses have robust security measures in place.

"Processes for rapid patching, keeping up to date with threat intelligence, testing systems for signs of compromise, and having an effective incident response plan in place can help organisations to be much better placed to identify and quickly resolve any issues."

To read the research update in full, please click here.

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 customers to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience, and investment in research and innovation, it is best placed to help organisations assess, develop and manage their cyber resilience posture.

With circa 2,000 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

Contacts

NCC Group Press Office
Press Contact
All media enquires relating to NCC Group plc
press@nccgroup.com
+44 7824 412 405
+44 7976 234 970