Threat Source newsletter (May 26, 2022) —— BlackByte adds itself to the grocery list of big game hunters

By Jon Munshaw.

Welcome to this week's edition of the Threat Source newsletter. Given the recent tragedies in the U.S., I don't feel it's appropriate to open by being nostalgic or trying to be witty —— let's just stick to some security news this week.

The one big thing

The BlackByte ransomware group uses its software for its own goals and as a ransomware-as-a-service offering to other criminals. This actor and its affiliates have infected victims all over the world, from North America to Colombia, the Netherlands, China, Mexico and Vietnam. BlackByte updated its leak site with a new design and new victims and is still actively exploiting victims worldwide.

Why do I care?

Talos has been monitoring BlackByte for several months and we can confirm they are still active after the FBI released a joint cybersecurity advisory in February 2022. Additionally, BlackByte is considered part of the big game ransomware groups, which are targeting large, high-profile targets, looking to exfiltrate internal data and threatening to publicly release it. Like similar groups, they have their own leaks site on the darknet.

So now what?

It's more important now than ever to have a multi-layered security architecture to detect these types of attacks. The adversary is likely to manage to bypass one of the other cybersecurity measures, but it is much harder for them to bypass all of them. There's also a ton of IOCs you can add to any block lists that we have listed on our blog, as well as previous Snort rules and ClamAV signatures to protect against this threat actor.

Other news of note

The ongoing battle between the Conti ransomware gang and Costa Rica continued this week, with Costa Rica's president saying his government is "at war" with Conti. Meanwhile, Conti seems to have dissolved and is now broken up between several sub-groups, though Conti actors continue to release statements on Costa Rica. This massive ransomware attack on a country's government has other smaller states worried they could be the next ransomware target. Many services in Costa Rica have been inoperable for weeks after the Conti attack. (Tech Monitor, The Verge, TechCrunch)

Several state-sponsored actors in Europe and the Middle East are buying the "Predator" spyware from commercial surveillance company Cytrox to spy on Android users. Researchers from Google say they've spotted these actors operating in Egypt, Armenia, Greece, Madagascar, Côte d'Ivoire, Serbia,

Spain and Indonesia. The firm sold the spyware along with exploits for zero-day vulnerabilities in the Chrome web browser and Android operating system, which are now all patched. (Google Threat Analysis Group, Gizmodo)

Zoom patched an XMPP vulnerability chain that could lead to remote code execution, along with several other security vulnerabilities in the virtual meeting client. A security researcher discovered an attack chain in which an attacker sends messages to the target over Zoom chat with the XMPP protocol —— no user interaction is required. If successful, the attacker could then execute remote code on the targeted machine. Other vulnerabilities Zoom disclosed this week included an issue that could allow an adversary to send user session cookies to a non-Zoom domain, which could allow for spoofing. (Security Week, Google Project Zero)

Can’t get enough Talos?

- Vulnerabilities in Open Automation Software Platform could lead to information disclosure, denial of service
- CTA Board of Directors Spotlight: Matt Watchinski, Cisco Talos
- People Behind CSR at Cisco: How JJ Cummings protects people in Ukraine from cyberthreats
- Threat Roundup for May 13 - 20
- Talos Takes Ep. #97: MustangPanda stays agnostic

Upcoming events where you can find Talos

REcon (June 3 — 5, 2022) Montreal, Canada

RSA 2022 (June 6 — 9, 2022) San Francisco, California

Cisco Live U.S. (June 12 — 16, 2022) Las Vegas, Nevada

Most prevalent malware files from Talos telemetry over the past week

SHA 256: e4973db44081591e9bff5117946defbef6041397e56164f485cf8ec57b1d8934 MD5: 93fefc3e88ffb78abb36365fa5cf857c Typical Filename: Wextract Claimed Product: Internet Explorer Detection Name: PUA.Win.Trojan.Generic::85.lp.ret.sbx.tg

SHA 256: 125e12c8045689bb2a5dcad6fa2644847156dec8b533ee8a3653b432f8fd5645 MD5: 2c8ea737a232fd03ab80db672d50a17a Typical Filename: LwssPlayer.scr Claimed Product: 梦想之巅幻灯播放器 Detection Name: Auto.125E12.241442.in02

SHA 256: 1fce2981e0d7d9c85adeea59a637d77555b466d6a6639999c6ae9b254c12dc6b MD5: f5d20b351d56605bbb51befee989fa6e Typical Filename: lavasoft_overlay_new_setup_progress_en.exe Claimed Product: PF001's Installer Detection Name: W32.8B439CC5BF-95.SBX.TG

SHA 256: 818d2d5bdde999f70563c16bfa9c724897d3b01adc67089137ae97d8f7ab6ba3 MD5: 9b1f8a838b5c195f9cf2f11017e38175 Typical Filename: document-launch-powershell.xls Claimed Product: N/A Detection Name: Auto.818D2D.242455.in02

SHA 256: 59f1e69b68de4839c65b6e6d39ac7a272e2611ec1ed1bf73a4f455e2ca20eeaa MD5: df11b3105df8d7c70e7b501e210e3cc3 Typical Filename: DOC001.exe Claimed Product: N/A Detection Name: Win.Worm.Coinminer::1201

Posted by Jon Munshaw at 2:00 PM Labels: Features, Threat Source newsletter Share This Post Facebook share Twitter share Linkedin share Reddit share Email This