Microsoft shares threat intelligence at CYBERWARCON 2023

microsoft.com/en-us/security/blog/2023/11/09/microsoft-shares-threat-intelligence-at-cyberwarcon-2023/

November 9, 2023

By

At the CYBERWARCON 2023 conference, Microsoft and LinkedIn analysts are presenting several sessions detailing analysis across multiple sets of threat actors and related activity. This blog is intended to summarize the content of the research covered in these presentations and demonstrates Microsoft Threat Intelligence's ongoing efforts to track threat actors, protect customers, and share information with the wider security community.

Reactive and opportunistic: Iran's role in the Israel-Hamas war

This presentation compares and contrasts activity attributed to Iranian groups before and after the October 7, 2023 start of the Israel-Hamas war. It highlights a number of instances where Iranian operators leveraged existing access, infrastructure, and tooling, ostensibly to meet new objectives.

With the physical conflict approximately one month old, this analysis offers early conclusions in a rapidly evolving space, specific to observed Iranian actors, such as those linked to Iran's Ministry of Intelligence and Security (MOIS) and Islamic Revolutionary Guard Corps (IRGC). While the presentation details attack techniques observed in specific regions, Microsoft is sharing this information to inform and help protect wider organizations around the world facing attack methods similar to those used by Iranian operators, such as social engineering methods for deceiving victims, and exploitation of vulnerable devices and sign-in credentials.

First, Microsoft does not see any evidence suggesting Iranian groups (IRGC and MOIS) had coordinated, pre-planned cyberattacks aligned to Hamas' plans and the start of the Israel-Hamas war on October 7. Although media and other public accounts may suggest that Iran played an active role in planning the October 7 physical attacks on Israel, Microsoft data tells a different part of the story.

Observations from Microsoft telemetry suggest that, at least in the cyber domain, Iranian operators have largely been reactive since the war began, exploiting opportunities to try and take advantage of events on the ground as they unfold. It took 11 days from the start of the ground conflict before Microsoft saw Iran enter the war in the cyber domain. On October 18, 2023 Microsoft observed the first of two separate destructive attacks targeting infrastructure in Israel. While online personas controlled by Iran exaggerated the claims of impact from these attacks, the data suggests that both attacks were likely opportunistic in nature. Specifically, operators leveraged existing access or acquired access to the first available target. Further, the data shows that, in the case of a ransomware attack, Iranian actors' claims of impact and precision targeting were almost certainly fabricated.

Second, Microsoft observes Iranian operators continuing to employ their tried-and-true tactics, notably exaggerating the success of their computer network attacks and amplifying those claims and activities via a well-integrated deployment of information operations. This is essentially creating online propaganda seeking to inflate the notoriety and impact of opportunistic attacks, in an effort to increase their effects. For example, Microsoft observed Iranian actors compromising connected webcams and framing the activity as more strategic, claiming they targeted and successfully compromised cameras at a specific Israeli military installation. In reality, the compromised cameras were located at scattered sites outside any one defined region. This suggests that despite Iran actors' strategic claims, this camera example was ultimately a case of adversaries continuing to opportunistically discover and compromise vulnerable connected devices and try to reframe this routine work as more impactful in the context of the current conflict.

Third, Microsoft recognizes that, as more physical conflicts around the world spur cyber operations of varying levels of sophistication, this is a rapidly evolving space requiring close monitoring to assess potential escalations and impact on wider industries, regions, and

customers. Microsoft Threat Intelligence anticipates Iranian operators will move from a reactive posture to more proactive activities the longer the current war plays out and continue to evolve their tactics in pursuit of their objectives.

The digital reality: A surge on critical infrastructure

In this presentation, Microsoft Threat Intelligence experts walk the audience through the timeline of Microsoft's discovery of Volt Typhoon, a threat actor linked to China, and the adversary group's activity observed against critical infrastructure and key resources in the U.S. and its territories, such as Guam. The presentation highlights some of the specific techniques, tactics, and procedures (TTPs) Volt Typhoon uses to carry out its operations. The talk features insights on how Microsoft tracked the threat actor and assessed that Volt Typhoon's activity was consistent with laying the groundwork for use in potential future conflict situations. These insights show the backstory of threat intelligence collection and analysis, leading to Microsoft's May 2023 blog on Volt Typhoon, sharing the actor's reach and capabilities with the community.

At CYBERWARCON, Microsoft provides an update on Volt Typhoon activity, highlighting shifts in TTPs and targeting since Microsoft released the May blog post. Specifically, Microsoft sees Volt Typhoon trying to improve its operational security and stealthily attempting to return to previously compromised victims. The threat actor is also targeting university environments, for example, in addition to previously targeted industries. In this presentation, Microsoft experts compare their Volt Typhoon analysis with third-party research and studies of China's military doctrine and the current geopolitical climate. This adds additional context for the security community on possible motivations behind the threat actor's current and future operations.

Microsoft also describes gaps and limitations in tracking Volt Typhoon's activity and how the security community can work together to develop strategies to mitigate future threats from this threat actor.

"You compile me. You had me at RomCom." – When cybercrime met espionage

For many years, the security community has watched various Russian state-aligned actors intersect with cybercrime ecosystems to varying degrees and with different purposes. At CYBERWARCON 2022, Microsoft discussed the development of a never-before-seen "ransomware" strain known as Prestige by Seashell Blizzard (IRIDIUM), a group reported to be comprised of Russian military intelligence officers. The cyberattack, disguised as a new "ransomware" strain, was meant to cause disruption while providing a thin veneer of plausible deniability for the sponsoring organization.

This year at CYBERWARCON, Microsoft experts profile a different threat actor, Storm-0978, which emerged in the early 2022 as credibly conducting both cybercrime operations, as well as espionage/enablement operations benefiting Russia's military and other geopolitical interests, with possible ties to Russian security services. The duality of this Storm-0978 adversary's activity intersecting with both crime and espionage leads to questions Microsoft are engaging conference attendees in exploring. Is Storm-0978 a cybercrime group conducting espionage, or a government-sponsored espionage group conducting cybercrime? Why are we seeing the confluence of what historically have been separate crime and geopolitical objectives? Is this duality in some way a reflection of Russia becoming limited in its ability to scale wartime cyber operations? Is Russia activating cybercriminal elements for operations in order to provide a level of plausible deniability for future destructive attacks? The Ukraine war has illustrated that Russia has likely had to activate other capabilities on the periphery. Storm-0978 is one probable example where it's clear that other elements have been co-opted to achieve objectives of both a wartime environment and strategic landscape either to achieve effects-led operations or prepositioning.

Microsoft's extensive insight on the ransomware economy and other cybercrime trends, coupled with experience tracking Russian nation-state adversaries, allows for presenting this profile of the Storm-0978 actor at CYBERWARCON, which Microsoft hopes will be further enriched and analyzed by the wider security community's experiences, data sets and conclusions.

A LinkedIn update on combating fake accounts

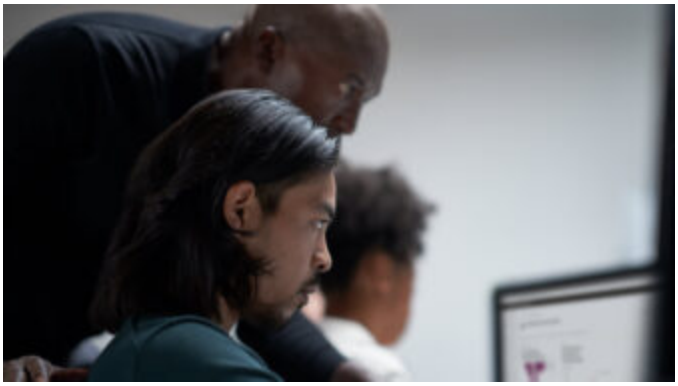
This presentation focuses on what LinkedIn's Threat Prevention and Defense team has learned from its investigations of cyber mercenaries, also referred to as private-sector offensive actors (PSOAs), on the platform. The focus of this presentation is on Black Cube (Microsoft tracks this actor as Blue Tsunami), a well-known mercenary actor, and what we've learned about how they attempt to operate on LinkedIn. The discussion includes insights on how Black Cube has previously leveraged honeypot profiles, fake jobs, and fake companies to engage in reconnaissance or human intelligence (HUMINT) operations against targets with access to organizations of interest and/or concern to Black Cube's clients.

Further reading

For the latest security research from the Microsoft Threat Intelligence community, check out the Microsoft Threat Intelligence Blog: https://aka.ms/threatintelblog.

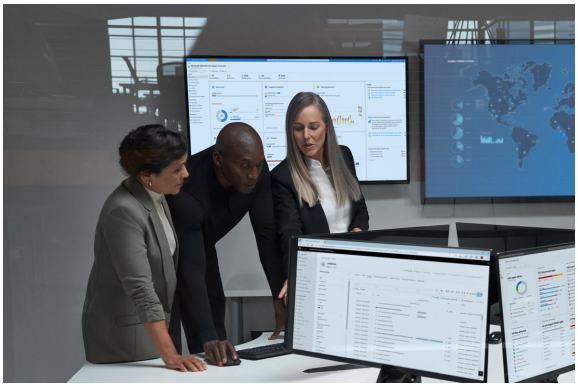
To get notified about new publications and to join discussions on social media, follow us on X at https://twitter.com/MsftSecIntel.

Related Posts



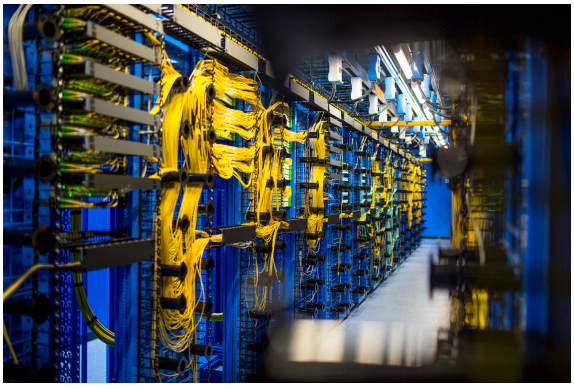
Peach Sandstorm password spray campaigns enable intelligence collection at high-value targets

Since February 2023, Microsoft has observed a high volume of password spray attacks attributed to Peach Sandstorm, an Iranian nation-state group. In a small number of cases, Peach Sandstorm successfully authenticated to an account and used a combination of publicly available and custom tools for persistence, lateral movement, and exfiltration.



Nation-state threat actor Mint Sandstorm refines tradecraft to attack high-value targets

Today, Microsoft is reporting on a distinct subset of Mint Sandstorm (formerly known as PHOSPHORUS), an Iranian threat actor that specializes in hacking into and stealing sensitive information from high-value targets. This subset is technically and operationally mature, capable of developing bespoke tooling and quickly weaponizing recently disclosed vulnerabilities.



New “Prestige” ransomware impacts organizations in Ukraine and Poland

The Microsoft Threat Intelligence Center (MSTIC) has identified evidence of a novel ransomware campaign attributed to IRIDIUM targeting organizations in the logistics and transportation industry in Ukraine and Poland utilizing a previously unidentified ransomware payload.