Threat Intel Report

Prepared by:

CBI Threat Intel Group

April 14, 2022

securityalert@cbisecure.com | 800.747.8585

With any security posture, visibility is important—knowing your environment, its activity, and where your data resides. But what about your data that lives *outside* your environment? That is, the data in the hands of companies whose services and tools you use.

Every organization employs third-party tools, from the largest enterprise to the smallest mom-and-pop shop. Larger organizations can have thousands of connections to external providers, while even the smallest businesses use third-party applications such as email, security solutions, or invoicing and payment processing systems. In every case, organizations must share a certain amount of data with these third-party providers. The question is how well that data is secured.

Supply chain attacks are on the rise, and the fallout can be devastating not only for the compromised organization but also for its customers and partners. Just as important as the data in your own environment is the data under the stewardship of your vendors, partners and suppliers.

Update on Ukraine

With the Russia-Ukraine war, nations and organizations worldwide have united to put pressure on Russia. Sanctions are being imposed, and we have also noticed an increase in cyber threat intelligence sharing among government and private organizations.

1200

Russian Soldiers Were Doxed by Hackivist Group, Anonymous

Threat actors, too, have taken sides. Shortly after Russia's invasion of Ukraine, Anonymous declared cyber war on the Putin regime. The hacktivist group has been responsible for bringing down several Russian government websites as well as doxing 120,000 Russian soldiers and leaking data from Russian entities. Meanwhile, the notorious Conti group publicly stated its alignment with Russia, leading to leaks of some of the group's deepest operating secrets and software.

As threat actors are known to do during events that grab the world's attention, various attacker groups are exploiting Ukraine's tragedy for profit. Preying on users' sympathies and emotions, these groups use phishing emails with Ukraine-related themes as hooks for spreading malware and stealing credentials and other information. Organizations should emphasize to employees the importance of validating and confirming seemingly humanitarian causes before subscribing or donating, whether using personal or employer devices or email services.

With the war's progression, many have speculated about the lack of a successful major Russian cyber attack on Ukraine. Mikko Hypponen, chief research officer at WithSecure, attributes this to Ukraine's proficiency in cyber defense after seven years of practice defending against such nation-state attacks. Earlier this month Ukraine rebuffed an attack on its energy infrastructure from the Russian state-sponsored hacking group Sandworm.

Third-Party Risks

A new report by NCC Group found that supply chain attacks increased by 51% in the last half of 2021. This finding is reminiscent of the words of Chinese General Sun Tsu: "If you know your enemies and know yourself, you will not be imperiled in a hundred battles; if you do not know your enemies but do know yourself, you will win one and lose one; if you do not know your enemies nor yourself, you will be imperiled in every single battle."

51%

Increased Supply Chain Attacks During the Last Half of 2021

Organizations spend considerable sums every month to understand their unique threats by investing in security systems, logging and monitoring solutions, and endpoint detection and response tools. Many companies also invest in threat intelligence to gain a deeper understanding of who their attackers are, why they are being targeted, and new attacker groups entering the scene.

But do we truly know ourselves if we don't know where our data resides outside our network, who has access to it, or how it is protected? Over the past few years, we have seen major supply chain compromises involving third-party vendors and partners, from tools that help provide visibility and manage environments such as Kaseya and SolarWinds, to financial and business contract management solutions such as Kronos. Most recently, the Lapsus$ compromise of a third-party contractor exposed 366 Okta customers.

A String of Lapsus$ Attacks

The Laspsus$ gang, reportedly led by a 16-year-old in the UK, was responsible for a recent string of hacks on large organizations using relatively unsophisticated methods. The group compromised companies such as Nvidia, Samsung, Microsoft and Okta.

To gain entry to organizations, Lapsus$ used tactics such as stealing credentials using malware; buying credentials on the dark web; SIM swapping to bypass MFA; social engineering via phone; and even paying employees inside organizations for credentials. Solid security best practices such as security awareness training; implementing strong MFA; and zero-trust architecture should be organizations' focus in preventing these types of attacks.

Nvidia

With its hack on Nvidia, Lapsus$ took the unconventional step of issuing a non-monetary ransom demand. Nvidia produces integrated and dedicated graphic cards used in computers around the world. These cards are highly popular with gamers, but with the rise in cryptocurrency values, crypto miners have also been buying them up, contributing to a shortage. In response, last year Nvidia implemented a technology that limits its cards' crypto mining capacity.

After hacking Nvidia in late February and leaking employee password hashes, Lapsus$ threatened to release more confidential corporate information unless Nvidia removed its crypto hash rate-limiting technology. The group then expanded the demand, ordering Nvidia to release its drivers as open source. The attackers later exposed Nvidia's code signing certificates, allowing threat actors to sneak past malware detection systems by signing malicious executables as if they were Nvidia proprietary software.

Microsoft

Microsoft had been following Lapsus$ for weeks before the tech giant itself became the hacker group's victim. According to Microsoft, the attackers gained access via a single account and accessed portions of source code (from Bing and Cortana) but no customer data. It was the hackers' own noisiness that allowed Microsoft to stop the group mid-operation: Lapsus$ announced its access to Microsoft on its Telegram channel while the group was exfiltrating data. The tipoff enabled Microsoft's threat intel team to intervene and stop the attack, limiting the damage.

2.5%

of Okta Clients Were Impacted by Lapsus$

Okta

After already having compromised several large organizations, Lapsus$ announced in March that it had compromised security authentication provider Okta. The group had obtained access by compromising the computer of a customer support engineer at Sitel, a subcontractor providing services to Okta. Lapsus$ released screenshots proving it had been within the Okta environment. Okta confirmed that 366 of its clients, or around 2.5% of its customer base, had been impacted.

According to the Department of Health and Human Services, the breach has resulted in the compromise of healthcare organizations. The HHS has since published a brief on the Lapsus$ hack of Okta to warn the health sector about the threat of attacks via managed service providers.

A Lapse in Lapsus$?

Lapsus$ was not especially careful to cover its tracks, and seven of its members, ranging in age from 16 to 21, have since been arrested. Activity from the group has also subsided for the time being.

Recommendations

To reduce the risk posed by third parties, organizations should catalog and then conduct assessments of all contractors, suppliers, and partners who may host data outside of your organization's environment. A third-party risk assessment is a valuable process for understanding the scope of cyber risks associated with suppliers, vendors and partners.

Contact the CBI Threat Intel Group at securityalert@cbisecure.com