EINPRESSWIRE

MSPs putting a stop to “hide and seek” within their environments with ESET Cloud Office Security

DUBAI , DUBAI, UNITED ARAB EMIRATES, January 16, 2024 /EINPresswire.com/ -- Roman Cuprik, Content Writer, ESET explains that amidst increased obfuscation of multistage malware attacks, MSPs need an effective way to secure cloud communication while avoiding the need for multiple unique network connection authorizations.

The days of simple and easily detectable malware are long gone. Recent campaigns by both OilRig and MuddyWater advanced persistent threat (APT) groups show that threat actors are constantly seeking new ways to hide their multistage malware attacks among files of commonly used cloud services.

This presents a dilemma for managed service providers (MSPs) that rely heavily on cloud-based solutions. But how should MSPs defend against increasingly sophisticated attacks without the burden of trying to control every single stream of communication within the MSP environment?

A growing market and a growing threat
With the never-ending hunger for cloud-managed services, it is no surprise that the MSP market is constantly expanding, and business reports, such as MarketsandMarkets, expect further growth by around $100 billion U.S. dollars within the next five years.

Both MSPs and other outsourced business practices have proven to be the answer for countless companies seeking high-end solutions for reasonable prices. But there are two sides to every coin. Professional communications, services, and shared files all moving to the cloud has created a new breeding ground for sophisticated malware.

Threat actors deploying this malware are often profit-driven and/or state-sponsored APT groups using command-and-control (C&C) servers to communicate with compromised devices over targeted networks. When successful, these servers can issue commands to steal or encrypt data, spread malware, disrupt web services, and more.

To enable this approach, APT groups need to establish persistence within the targeted businesses, obfuscating malicious files and processes among legitimate ones.

A draft email one will never send … nor ever even wrote

ESET researchers have described recent attacks in detail while following the evolution of campaigns run by the OilRig group.

To avoid cybersecurity scanning tools, OilRig has not been deploying fully fledged malware but, instead, has scaled its attacks. While the initial attack vector of the recent campaigns remains unknown, presumably it was a phishing email. This email would contain a downloader that wouldn't cause any specific damage but, as the name implies, is designed to secretly download additional malware from the internet. Several versions of these downloaders have been documented by ESET researchers.

Studying these downloaders, it is clear that OilRig is keenly focused on identifying new ways to obfuscate malware deployment using legitimate cloud service providers for C&C communication.

The first in the series, SC5k downloader, uses the a shared Microsoft Exchange email account and Microsoft Office Exchange Web Services API for C&C communication. Within this email account, the attackers create draft messages with hidden commands. Once the downloader infests a device, it will log in to the same account to receive both the commands and the payloads to execute. Its successor, OilCheck, works similarly but uses the Outlook mail API in Microsoft Graph.

New versions of OilRig downloaders, ODAgent and OilBooster, communicate using the Microsoft Graph OneDrive API. They access a OneDrive account controlled by the attackers for C&C communication and exfiltration.

The evolution of malware-hiding capabilities was also recently noted in the case of another APT group linked to Iran called MuddyWater.

In a separate MuddyWater campaign, described by DeepInstinct, the APT group reused previously known remote administration tools and hid them in the cloud-based content management system (CMS), called Storyblok, to host archives with compromised files.

ESET to help deal with the dilemma

The hiding capabilities of present-day C&C attacks have pushed businesses toward higher control over their network traffic. From standard network monitoring, it can go as far as individually authorizing any network connection.

However, the higher the control, the higher the workload on MSP admins and technicians who are already drained from a never-ending stream of alerts. So what do businesses choose: strict control that comes with alert fatigue or lower security standards that can result in a data breach?

With its MSP Program, ESET can help businesses deal with this dilemma. The program is based on the ESET PROTECT solution, which provides multilayered protection, and its higher tiers also integrate ESET Cloud Office Security (ECOS), which is designed to protect Microsoft 365 and Google Workspace applications.

ECOS — effectiveness in numbers*
750,000 email threats detected
360,000 phishing emails blocked
21 million spam emails captured
*7-month period in 2023

In fact, these ESET security solutions can disrupt the described C&C processes at several stages, which means that companies don’t have to focus on network control as much.

Anti-phishing protection

Though the initial attack vectors of OilRig and MuddyWater campaigns are unknown, both APT groups have successfully kicked off their campaigns with phishing emails in the past. ECOS prevents users from accessing web pages known for phishing once they click on the phishing link in the email.

Antimalware protection

ESET’s defense against malware eliminates all types of threats. Moreover, ECOS scans all new and changed files in OneDrive, Google Drive, Microsoft Teams, and SharePoint Online.

ESET LiveGuard Advanced

If ESET malware detection engines detect a never-before-seen type of threat, they pass the file to the ESET cloud-based sandboxing tool ESET LiveGuard Advanced for further assessment.

Multi-tenant

ECOS multi-tenant functionality protects and manages multiple Microsoft 365 and Google Workspace tenants from one ESET Cloud Office Security console.

Conclusion

The growth of cloud-based business practices has ushered in cloud-based cyberattack tactics that MSPs need to deal with. And the results can be dire. With their privileged access to business networks, compromised MSPs can also be dangerous for their clients by triggering a supply chain attack.

The good news is that one does not need to face those threats alone. Since its foundation in 1992, ESET has developed a robust multilayered defense system capable of stopping C&C attacks at different stages and much more. ESET solutions are also available for MSPs as a part of the ESET MSP Program. Don’t be the weak link in supplier relationships. Be the strongest.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here