SecurityScorecard

CYBER RISK INTELLIGENCE

SecurityScorecard Analysis of Traffic Involving Storm-0558 IoCs

Executive Summary

On July 11th, 2023, Microsoft disclosed that a threat actor had obtained a Microsoft private encryption key that allowed attackers to generate tokens enabling access to customers' Exchange Online and Outlook[.]com accounts.

Subsequent research found that the compromised key could have granted access to a wider variety of applications including Azure Active Directory, SharePoint, Teams, and OneDrive.

The SecurityScorecard Threat Research, Intelligence, Knowledge, and Engagement (STRIKE) Team consulted a strategic partner's traffic data as well as public reporting on the incident to offer further insight into these claims.

STRIKE Team researchers identified a collection of IP addresses through which attackers may have communicated with those Microsoft named as indicators of compromise (IoCs).

Background

On July 11th, 2023, Microsoft disclosed that a threat actor had obtained a Microsoft private encryption key that allowed attackers to generate tokens enabling access to customers' Exchange Online and Outlook.com accounts. Microsoft attributed the attack to a threat actor group it tracks as Storm-0558, which it assesses conducts espionage on behalf of the People's Republic of China.

Despite some similarities between it and more established Chinese APTs (namely the group tracked as Violet Typhoon, ZIRCONIUM, and APT31), Microsoft assesses that Storm-0558 is likely a distinct operation.

The group's targets have, thus far, been fairly typical for a Chinese APT group. They include US and European government agencies, parties linked to Taiwanese and Uyghur causes, media companies, think tanks, and telecommunications equipment and service providers. The group's main focus has been email account access, which the recent activity's apparent interest in Outlook would also reflect. Microsoft reported that in these attacks, Storm-0558 had accessed email accounts belonging to 25 organizations, including government agencies and other consumer accounts belonging to individuals seemingly linked to the target agencies, beginning on May 15.

In this most recent campaign, the group first used the SoftEther VPN when accessing its targets, but later began using dedicated servers to communicate with target assets. Microsoft additionally noted that the group had routed some of its traffic through TOR proxies or SOCKS5 proxy servers. The IoCs Microsoft published included the IP addresses for both types of infrastructure and the timeframes in which Storm-0558 used each IP address.

Following the publication of Microsoft's analysis, another firm released the results of its investigation into the campaign on July 21. According to its findings, the compromised key could have granted attackers access to a wider variety of applications than just Exchange Online and Outlook[.]com, including both Microsoft-managed applications such as SharePoint, Teams, and OneDrive. Additionally, customer-managed applications that permit authentication via Microsoft account (i.e. those with a "Log in with Microsoft" feature) could have been accessed. This could suggest that the compromise affected more organizations than the 25 that Microsoft originally estimated.

Findings

The traffic data available to SecurityScorecard suggests that Storm-0558 may have used the following IP addresses (which communicated with those Microsoft named as IoCs) to access the dedicated servers through which they then interacted with target assets:

- 103.188.48[.]31
- 103.143.143[.]105
- 195.176.19[.]2
- 103.83.158[.]7
- 172.68.47[.]74
- 103.160.62[.]167
- 104.236.242[.]206
- 67.21.86[.]202
- 34.104.35[.]123
- 192.42.116[.]213

While the available traffic samples offered few novel insights into the campaigns' victimology, some of the data they contain may support the previous observations made regarding Storm-0558's targeting, as they suggest targeting of both Microsoft and European government agencies. While IP addresses belonging to many telecommunications services and hosting providers appear in the samples, researchers were unable to identify which particular customers (if any) used these IP addresses during the sampling periods. Although some of this traffic could indicate targeting of telecommunications firms themselves—given that Microsoft has noted that Storm-0558 has previously targeted telecommunications firms—the available data does not necessarily lend itself to this conclusion, as the traffic could reflect communication involving (as yet unknown) telecommunications service providers' customers rather than the services providers themselves. However, one IP address registered to Microsoft and nine IP addresses registered to a Western European government ministry communicated with the IP addresses that Microsoft named as IoCs. Although these communications involved the IoCs Microsoft identified as belonging to the SoftEther VPN) and could therefore reflect communications between other VPN users and the possible target organizations), given the available reports regarding Storm-0558's targeting, this activity could suggest targeting of these organizations, given that they fall within the sectors named as previous Storm-0558 targets.

Methodology

Researchers leveraged SecurityScorecard's unique access to network flow (NetFlow) data to collect traffic samples for the IP addresses Microsoft listed as IoCs in its report. They collected a separate sample for each IP address using the ranges of dates Microsoft provided.

To identify those IP addresses in the traffic samples that appeared most likely to be ones the attackers had used to access those named as IoCs before launching further activity through them, researchers focused on the traffic samples for the IP addresses named as dedicated servers. This was done assuming that traffic involving them was more likely to represent activity particular to Storm-0558 while traffic involving the IP addresses belonging to a VPN could be more likely to reflect activity by other users in addition to the threat actors. They next excluded IP addresses that SecurityScorecard's NetFlow data provider has linked to scanning or bot activity, as traffic involving those IP addresses is often quite indiscriminate and would be less likely to reflect concerted activity. They then searched for the remaining IP addresses in SecurityScorecard's Attack Surface Intelligence tool and public cybersecurity information-sharing platform VirusTotal to identify those that might have other characteristics named by Microsoft (for example, those other researchers have identified as TOR nodes). After that, they compared different traffic samples to identify the IP addresses that communicated with multiple dedicated servers. This was done assuming that those IP addresses that appear in multiple servers' traffic samples and do not represent scanning or other indiscriminate activity may be more likely to be IP addresses the threat actors used to connect to the dedicated servers discussed in Microsoft's report. Nine of the IP addresses listed above appeared in multiple traffic samples and one has been identified as a TOR exit node.

To identify the IP addresses that may represent targets of the recent Storm-0558 activity, researchers collected IP WHOIS data for all of the IP addresses in the traffic samples and selected those registered to Microsoft or organizations in sectors Storm-0558 has previously targeted.

Conclusion

Storm-0558's activity does not appear to have the disruptive potential of other recently-reported activity attributed to Chinese APT groups. That said, it and its possible impacts may nonetheless merit continued attention, given the reaction provoked not only by the attack, but also Microsoft's response to it. While the available NetFlow data may offer further insights into Storm-0558's recent activity targeting Microsoft's public cloud, certain limitations merit consideration. Although much of the commentary reacting to Microsoft's initial reporting on the campaign has revolved around its extent, with considerable attention dedicated to the possibility that it affected a larger number of organizations than the 25 Microsoft identified, the traffic samples do not lend themselves to clear conclusions regarding the scope of the campaign. The number of Microsoft IP addresses appearing in the samples was unexpectedly small and many of the IP addresses that did appear in the sample (those discussed above, which belong to telecommunications and hosting providers) offered few insights as to what organization was using them at the time the traffic samples were collected. Despite these limitations, the findings may offer some additional insight into the group's tactics, techniques, and procedures (TTPs), as the IP addresses listed above may have served as proxies through which attackers connected to the dedicated servers where they conducted some of the reported activity. Monitoring their resources for communication with these IP addresses, in addition to those previously named as IoCs, may therefore help organizations in target sectors better defend themselves.

SecurityScorecard.com
info@securityscorecard.com

United States: (800) 682-1707
International: +1(646) 809-2166