Intelligence Insights: January 2022

By susannah.matt@redcanary.com

Archived: 2026-04-05 19:38:10 UTC

⬆ = trending up from previous month
⬇= trending down from previous month
➡ = no change in rank from previous month

*Denotes a tie

Observations on trending threats

For the fourth consecutive month, we have a new threat at the top of our prevalence rankings. This time SocGholish made the ascent. The emergence of BLISTER malware as a follow-on payload (more on that below) may be related to this rise, and the 1.8% of customers affected is SocGholish's high water mark for the year.

Cobalt Strike, a mainstay of the top five spots every month this year, curiously dropped all the way down to the twelfth spot. Only ~0.5% of customers saw Cobalt Strike detections in December, after 11 straight months of over 1% seeing Cobalt Strike, with a peak of 3.2% of customers back in June. It remains to be seen if this represents a shift in tooling or TTPs by adversaries, or if this was merely a holiday lull for both red teamers and post-exploitation adversaries. In any case, Red Canary detection engineers are maintaining a vigilant watch on these and other threats.

New Conficker detection analytic identifies old persistence. Speaking of expanded detection coverage, you may have noticed Conficker, that years-old nuisance, creeping into the bottom of our rankings. This is not a re-emergence of a new threat, but an artifact of deploying a new detection analytic to shine a light on an old persistence technique hidden in a dark, and often overlooked, corner. In most instances, the malicious DLL payload of these Conficker cases was likely removed by antivirus long ago. However, the lingering persistence mechanism attempting to launch those randomly named libraries tends to languish in the labyrinth of the registry long after antivirus declares the threat removed. Expanding detection coverage does not just uncover new and novel threats, it also adds layers of defenses to ensure more complete and thorough clean-up of the closed out cases of the past.

Accordingly, we can add Conficker to the compendium of older threats with worming capabilities that are still finding their way into places they don't belong. If you're seeing Conficker detections, one way to harden your attack surface is to ensure you're running an up-to-date OS. You may also want to consider disabling AutoRun and checking over those firewall rules one last time, just to make sure you aren't haunted by any residual Conficker infections wandering about come the next holiday season.

Detection opportunity: Rundll32 executing with command lines consistent with Conficker

process_ name == `rundll32.exe`
&&
command_line_contains == `rundll32\.exe [a-z]{5,8}\.[a-z]{1,3},[a-z]{5,8}`

Note: *If you are having trouble getting this detection opportunity to work in your environment, you may find additional success by focusing only on processes where* `taskeng.exe` *or* `svchost.exe` *are the parents of* `rundll32`.

Adversaries find a juicy Log4j target in VMware Horizon

Since public disclosures of the Log4j vulnerabilities began on December 9, we've been tracking threats that have exploited them. We realized the attack surface using Log4j was huge, but in the first several weeks, the activity we observed consisted mostly of scanning, testing, and coinminers.

Detection opportunity: PowerShell listing VMBlastSG service names

This analytic identifies PowerShell executing a command to return a list of service names containing `VMBlastSG`. This may assist in identifying post-exploitation as described in this excellent NHS alert, similar to the following, which invokes `Get-WMIObject` on `win32_service` to return service names:

```
powershell -c "$path=gwmi win32_service|?{$.Name -like """VMBlastSG"""}|%{$.PathName -replace '"""', '' -replace """nssm.exe""","""lib\absg-worker.js"""}
```

process_name== `powershell.exe`
&&
command_line_contains == `VMBlastSG`

The nature of recently disclosed Log4j vulnerabilities may have contributed to the volume and delayed timing of activity observed in the wild. One of the reasons we did not observe a large volume of exploitation in the first few days may be that these vulnerabilities are highly application-specific, depending on how Log4j is implemented in them. This means an adversary could not have crafted a single exploit that would have had a broad impact on many types of applications at once.

Toward late December and early January, however, we observed an uptick in adversaries exploiting internet-facing VMware Horizon servers running versions affected by the Log4J vulnerabilities. While we couldn't attribute all activity to named adversaries, we observed likely PROPHET SPIDER activity in one environment, and patterns suggesting a potentially different adversary in other environments. Others in the community, including the UK NHS and Microsoft, observed the same pattern of adversaries targeting VMware Horizon. This supplements earlier reporting about Conti ransomware operators exploiting VMware vCenter during lateral movement in an environment. When viewed together, this reporting and our direct visibility suggests VMware Horizon is a top choice for adversaries to narrow their Log4j targeting, likely because it is widely used and often internet-facing. **We recommend everyone using VMware Horizon immediately apply updates and evaluate whether it needs to be internet-facing.**

SocGholish causing BLISTERs?

In December, Elastic Security published research exposing BLISTER, a newly discovered loader that may contain Cobalt Strike beacons or other remote access tools. This threat evades static signatures by splicing malicious code into a legitimate Windows executable while preserving most of the original executable's structure and content. Elastic observed BLISTER coming from malicious installers, and we observed a slightly different pattern: SocGholish deploying BLISTER. In at least one instance in December, we observed SocGholish deploying BLISTER, which deployed a Cobalt Strike beacon.

This development shows that **adversaries are actively using multiple methods to distribute BLISTER** and its subsequent payloads. BLISTER itself is evasive, hindering static analysis and detection rules.

Managing the increase in ManageEngine vulnerabilities

In December 2021, Red Canary observed activity associated with the likely exploitation of vulnerabilities in two Zoho ManageEngine products: ADSelfService Plus and ServiceDesk Plus. The FBI also reported in-the-wild exploitation of a vulnerability in a third ManageEngine product, Desktop Central. Given the frequency with which vulnerabilities in ManageEngine have been recently disclosed and the speed at which adversaries can exploit these newly reported weaknesses, Red Canary focuses on identifying and detecting post-exploitation behavior, and we recommend others do the same to identify malicious activity, regardless of how adversaries accessed the environment.

Detection opportunity: Java.exe writing msiexec.exe to disk

process_name == `java.exe`
file_modification == `msiexec.exe`

ADSelfService Plus (CVE-2021-40539)

As noted previously in our December Intelligence Insights, we've consistently observed operators dropping web shells and using `keytool.exe`, a Java utility, after exploiting what appears to be CVE-2021-40539. Separately, in one incident response engagement, our partner observed a ransomware attack after operators gained initial access via exploitation of CVE-2021-40539.

ServiceDesk Plus (CVE-2021-44077)

We've also observed CVE-2021-44077, a vulnerability in ManageEngine ServiceDesk Plus, likely exploited to upload a malicious executable and conduct post-exploitation reconnaissance. Behavior exploiting this vulnerability—in concert with a binary masquerading as `msiexec.exe`—appears to overlap with the TiltedTemple campaign recently reported by researchers at Palo Alto Unit 42.

Desktop Central (CVE-2021-44515)

The FBI released a FLASH notification detailing APT exploitation of a third ManageEngine vulnerability, this time in a Desktop Central MSP server, part of ManageEngine's Desktop Central product. Following successful exploitation of this vulnerability, the FBI reported that adversaries drop a web shell, conduct reconnaissance, and use BITSAdmin to download additional tools.

Though Red Canary has not observed successful exploitation of this vulnerability first-hand, credible reporting from CISA and the FBI highlights the risks associated with the follow-on activity successful exploitation can enable. Tracking public reporting on vulnerabilities such as CVE-2021-44515 allows us to add context to threats associated with common software and tailor our detection coverage to cover tradecraft highlighted by other sources in the community.

ManageEngine products are widely used among IT departments, presenting a large attack surface for adversaries. Organizations using ManageEngine products in their environment should update accordingly. Patches for all of the vulnerabilities listed here have been released and are available via ManageEngine.

As always, the assessments in this report represent our best thinking based on our current visibility. To this end, we welcome the receipt of conflicting or contradictory information on these threats and acknowledge that our assessments are subject to change over time as we incorporate new information. To submit additional information for consideration, please contact intel@redcanary.com.
