North Korean hackers stole research data in two-month-long breach

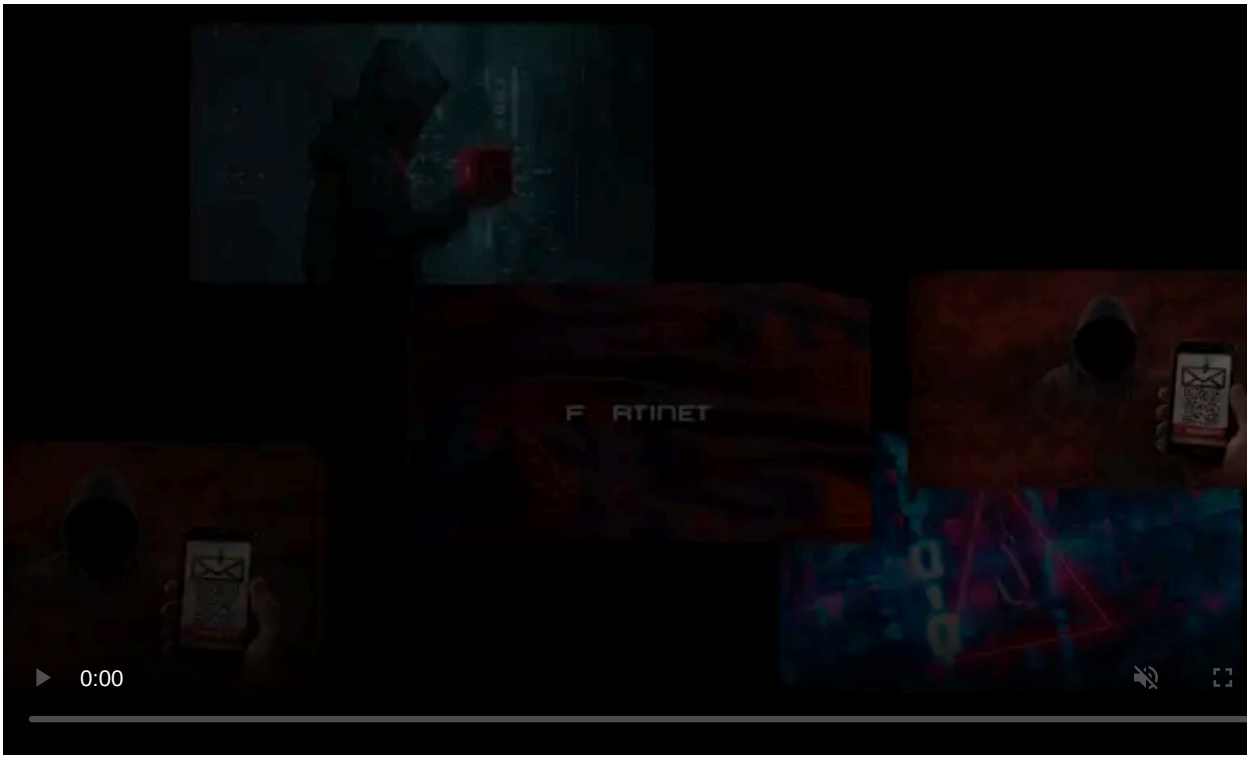
By Bill Toulas

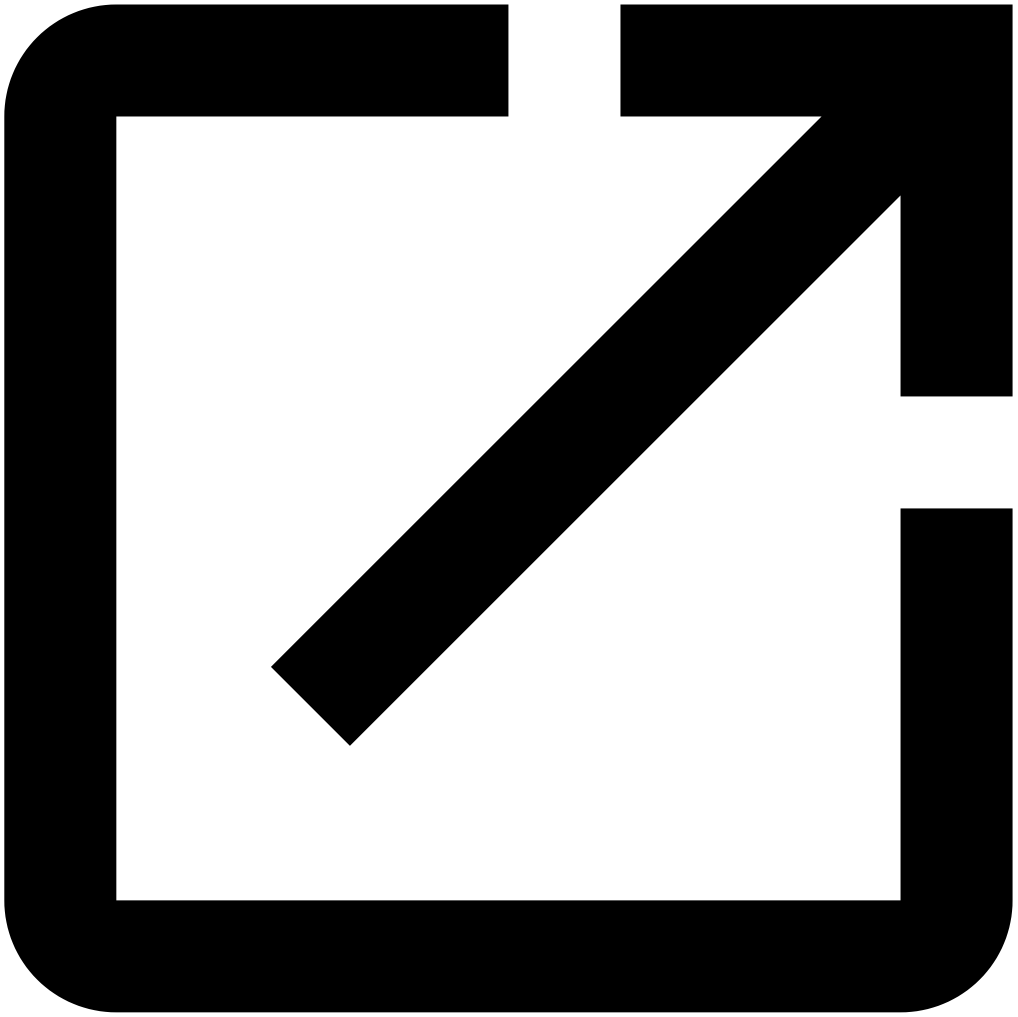
Published: 2023-02-02 · Archived: 2026-04-05 20:48:32 UTC

A new cyber espionage campaign dubbed 'No Pineapple!' has been attributed to the North Korean Lazarus hacking group, allowing the threat actors to stealthily steal 100GB of data from the victim without causing any destruction.

The campaign lasted between August and November 2022, targeting organizations in medical research, healthcare, chemical engineering, energy, defense, and a leading research university.

The operation was discovered by Finnish cybersecurity firm WithSecure, whose analysts were called to investigate a potential ransomware incident on one of its customers. However, thanks to an operational mistake by Lazarus, they were able to link the campaign to the North Korean APT.


F RTINET
0:00



WithSecure was able to attribute the activity based on multiple pieces of evidence but also noticed some new developments for Lazarus, like:

- the use of new infrastructure using IP addresses without domain names,
- a new version of the Dtrack info-stealer malware,
- a new version of the GREASE malware used in admin account creation and protection bypass.

The campaign is named after the '< No Pineapple! >' error seen transmitted by a remote access malware when uploading stolen data to the threat actor's servers.

Quietly stealing data

The Lazarus hackers compromised the victim's network on August 22nd, 2022, by leveraging the CVE-2022-27925 (remote code execution) and CVE-2022-37042 (authentication bypass) Zimbra vulnerabilities to drop a webshell on the target's mail server.

This RCE flaw was patched in May 2022, but the authentication bypass took Zimbra until August 12th to release a security update. By that time, it was already under active exploitation by threat actors.

After successfully breaching the network, the hackers deployed the tunneling tools 'Plink and '3Proxy' to create reverse tunnels back to the threat actors' infrastructure, allowing the threat actors to bypass the firewall.

Less than a week after, WithSecure says the intruders began utilizing modified scripts to extract approximately 5GB of email messages from the server and save them to a locally stored CSV file, which was later uploaded to the attacker's server.

Over the next two months, the threat actors spread laterally through the network, acquiring administrator credentials and stealing data from devices.

While spreading through the network, Lazarus deployed multiple custom tools, such as Dtrack and what is believed to be a new version of the GREASE malware, used to locate Windows administrator accounts.

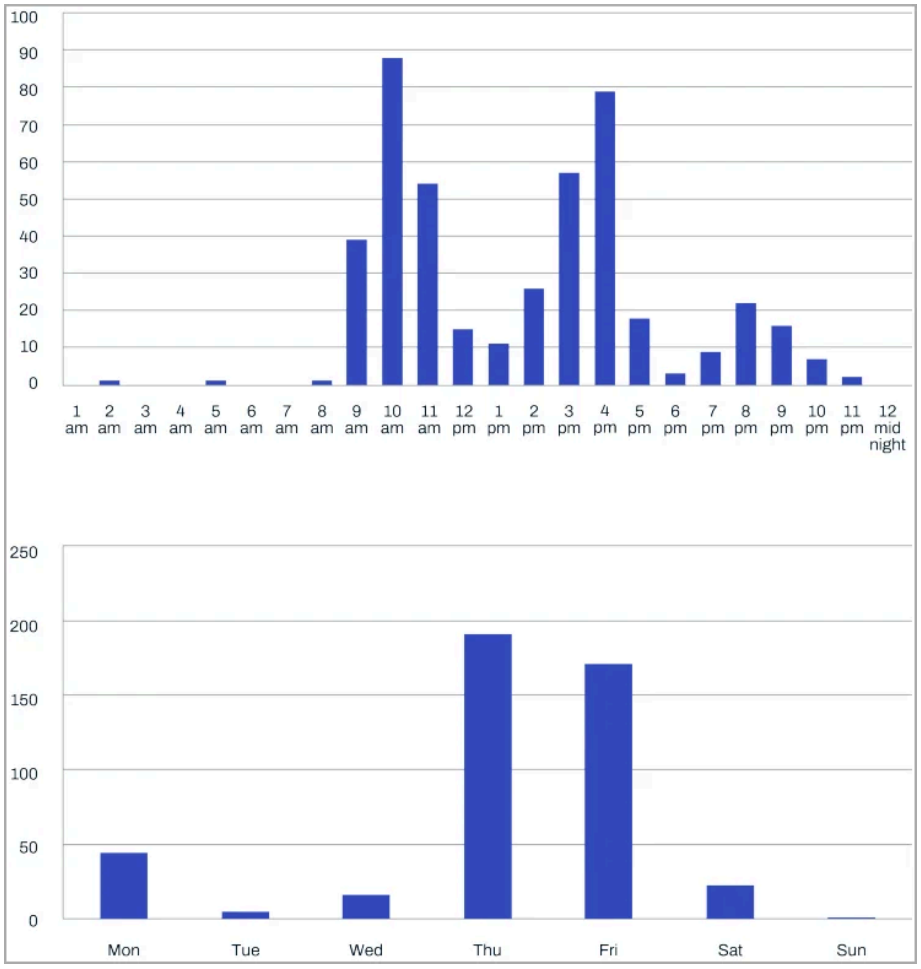
Dtrack is an information-stealing backdoor known to be used by Lazarus, while the GREASE malware is associated with Kimusky, another North Korean state-sponsored hacking group.

The attack culminated on November 5th, 2022, with the actors lurking in the network for over two months and ultimately stealing 100GB of data from the compromised organization.

WithSecure was able to analyze the work patterns of the threat actors, stating that they worked Monday through Saturday from 9 AM to 10 PM.

"Time zone attribution analysis concluded that the time zone aligns with UTC +9. Reviewing activity by time of day finds that most threat actor activity occurred between 00:00 to 15:00 UTC (09:00 and 21:00 UTC +9)," shared WithSecure.

"Analysing activity by day of the week suggests that the threat actor was active Monday to Saturday, a common work pattern for DPRK."



Lazarus working times and days in the recent campaign *(WithSecure)*

New malware and tactics

The first notable change found in this Lazarus campaign is that they now rely solely on IP addresses without domain names for their infrastructure.

This change has advantages for the threat actors, including reduced need for renewal maintenance and greater IP flexibility.

The new Dtrack variant spotted in the recent Lazarus attacks is dropped by an executable named 'onedriver.exe,' and it no longer uses its own C2 server for data exfiltration.

Instead, it relies on a separate backdoor to transfer the data it has gathered locally on the compromised machine, storing them in a password-protected archive.

"The staging and exfiltration host was likely carefully chosen by the threat actor to be a host where endpoint security monitoring tools were not deployed," explains WithSecure in the report.

The new GREASE malware used by Lazarus is executed on the host as a DLL ("Ord.dll") with higher privileges achieved by exploiting the 'PrintNightmare' flaw.

Its main difference compared to previous versions is that it now uses RDPWrap to install an RDP service onto the host to create a privileged user account with the help of net user commands.

Exposed by errors

Even for highly sophisticated threat actors like Lazarus, making mistakes isn't unheard of, and in this case, allowed the campaigns to be attributed to the hacking group.

WithSecure's investigation of retrieved network logs from the victim revealed that one of the web shells planted by the intruders was communicating with a North Korean IP address ("175.45.176[.]27").

This isolated incident occurred at the beginning of that day, preceded by connections from a proxy address, indicating that the threat actor likely exposed themselves by an error at the start of their workday.

Additionally, WithSecure observed that various commands executed on the breached network devices were very similar to those hardcoded inside Lazarus malware but often contained mistakes and didn't execute, indicating that the threat actors were typing them manually using the Impacket 'atexec' module.

Apart from the mistakes, WithSecure was able to link these operations to Lazarus based on TTP overlaps detailed in previous reports by Symantec and Cisco Talos, the employed malware strains, the profiles of the targets, infrastructure overlaps, and time-zone analysis.

WithSecure's report is another indication of Lazarus' activity, with the threat group continuing its efforts to gather intelligence and exfiltrate large amounts of data from high-profile victims.

Source: https://www.bleepingcomputer.com/news/security/north-korean-hackers-stole-research-data-in-two-month-long-breach/