KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | DEV-0569 Expands Toolkit Delivers Royal Ransomware

Tracker ID: TN1122 **Date:** 29/Nov/2022 **Category:** Malware **Industry:** All **Region**: All

Background

Along with the newly revealed Royal ransomware, a threat campaign was detected that used Google Ads to deliver multiple post-compromise payloads. The current malware distribution mechanism is part of the DEV-0569 group, whose attacks exhibit a pattern of constant innovation, with regular integration of innovative discovery techniques, defensive evasion, and varied post-compromise payloads, as well as increased ransomware facilitation. The threat actor employs the malvertising technique to drive naïve victims to malicious links that appear to be software installers for legitimate apps such as Adobe Flash Player, AnyDesk, LogMeIn, Microsoft Teams, and Zoom.

DEV-0569 can deliver its initial payload in a variety of ways. The payloads are sometimes supplied via phishing campaigns operated by other malicious actors who provide malware payload distribution as a service. The attack usually begins with a malicious link supplied to the victim via malicious advertising, fake forum pages, blog comments, or phishing emails. These URLs lead to malicious files signed with a valid certificate by the attacker. The malicious programs, known as BATLOADER malware downloaders, masquerade as installers or updates for genuine software such as Microsoft Teams or Zoom.

When launched, BATLOADER uses MSI Custom Actions to launch malicious PowerShell activity or run batch scripts to aid in disabling security solutions and lead to the delivery of various encrypted malware payloads that are decrypted and launched with PowerShell commands. Once launched, BATLOADER employs MSI Custom Actions to initiate malicious PowerShell activities or runs batch scripts to aid in the disabling of security solutions and delivers various encrypted malware payloads that are decrypted and launched with PowerShell commands.

DEV-0569 leveraged several infection chains, including PowerShell and batch scripts, to download malware payloads such as information stealers or an authentic remote management tool used for network persistence. The management tool might potentially be used as a ransomware staging and distribution hub. Furthermore, NSudo is used to launch applications with elevated privileges and compromise security by adding registry entries that disable antivirus protection.

DEV-0569's distribution vectors have been diversified via the use of Google Ads to distribute BATLOADER to specific people, allowing it to access more targets and disseminate malware payloads. It positions the gang to operate as an initial access broker for other ransomware operations, alongside malware such as Emotet, IcedID, and Qakbot. Because DEV-0569's phishing scheme exploits legitimate services, organizations should utilize mail flow rules to capture suspicious keywords or review broad exclusions, such as those connected to IP ranges and domain-level allow lists..

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

This document is for e-communication only.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | DEV-0569 Expands Toolkit
Delivers Royal Ransomware

Tracker ID: TN1122 **Date:** 29/Nov/2022 **Category:** Malware **Industry:** All **Region**: All

MITRE ATT&CK Tactics

Initial Access, Discovery, Execution, Defense Evasion.

Recommendations

- Check with your existing AV/EDR vendor to validate the detection scope of identified samples.
- Implement regular phishing awareness and training throughout the workplace. Make sure employees are aware of any active phishing threats.
- Verify the email sender and content before downloading attachments or selecting embedded links from emails. Hover the pointer above embedded links to show the link's target.
- Check the sender's identity. Unfamiliar email addresses, mismatched email and sender names, and spoofed company emails are some of the signs that the sender has malicious intent.
- Do not download file from unknown websites without verifying their legitimacy.
- Identify and remove suspicious registry values that try to disable antivirus solutions.
- As a protective measure, prevent unnecessary PowerShell execution by implementing policies and standards that permit only signed scripts to execute.
- Implement principle of least-privilege and maintain credential hygiene. Avoid the use of domain-wide, admin-level service accounts.
- Restricting local administrative privileges can help limit installation of RATs and other unwanted application.
- Continuously monitor for suspicious or anomalous activities. Collect and review relevant logs, data, and artifacts to identify any threat in the network.
- Follow multilayered defense solutions and active monitoring to detect threats before operators can launch their attacks.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

This document is for e-communication only.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | DEV-0569 Expands Toolkit Delivers Royal Ransomware

Tracker ID: TN1122 **Date:** 29/Nov/2022 **Category:** Malware **Industry:** All **Region**: All

References

- Microsoft Security Threat Intelligence, DEV-0569 finds new ways to deliver Royal ransomware, various payloads, Microsoft, 17th November 2022, External Link (www.microsoft.com).
- Shunichi Imano, Ransomware Roundup: Royal Ransomware, Fortinet, 13th October 2022, External Link (www.fortinet.com)
- Ravie Lakshmanan, Microsoft Warns of Hackers Using Google Ads to Distribute Royal Ransomware, The Hacker News, 19th November 2022, External Link (thehackernews.com)

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176471471

*

SHA256 Hash
2598e8adb87976abe48f0eba4bbb9a7cb69439e0c133b21aee3845dfccf3fb8f
9db958bc5b4a21340ceeeb8c36873aa6bd02a460e688de56ccbba945384b1926

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

This document is for e-communication only.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia