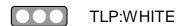


# **THREAT BULLETINS**

# New Sophisticated Email-Based Attack from NOBELIUM





May 28, 2021

On May 27, 2021, Microsoft issued an alert regarding an active wide-scale malicious email-based campaign operated by threat actor group NOBELIUM uncovered by the Microsoft Threat Intelligence Committee (MSTIC). NOBELIUM has been linked to the attacks against SolarWinds which included the SUNBURST backdoor, TEARDROP malware, GoldMax malware, and other related components.

The campaign, initially observed and tracked by Microsoft since January 2021, evolved over a series of waves demonstrating significant experimentation. On May 25, 2021, the campaign escalated as NOBELIUM leveraged the legitimate massmailing service, Constant Contact, to masquerade as the United States Agency

for International Development (USAID) and distribute malicious URLs to a wide variety of organizations and industry verticals.

With this latest attack, NOBELIUM attempted to target approximately 3,000 individual accounts across more than 150 organizations, employing an established pattern of using unique infrastructure and tooling for each target, increasing their ability to remain undetected for a longer period of time.

Please see the full report for additional information including malicious user redirection activity, detection details, advanced hunting, and observed MITRE ATT&CK techniques available here.

Upon initial discovery of the campaign in February, MSTIC identified a wave of phishing emails that leveraged Google's Firebase platform to stage a malicious ISO file, while also recording attributes of those who accessed the link. MSTIC traced the start of the campaign to January 28, 2021, when the actor appeared to be performing early reconnaissance by only sending the tracking portion of the email. During this time, no delivery of malicious payloads was observed.

Over a series of evolving delivery techniques, MSTIC observed NOBELIUM attempting to compromise systems using numerous methods. One of which included the use of an HTML file attached to a spear-phishing email that executed malicious JavaScript code when opened by the targeted user. From here, a shortcut file (LNK) would execute an accompanying DLL, which would result in Cobalt Strike Beacon executing on the system.

Experimentation continued through most of the campaign but began to escalate in April 2021. During the waves in April, the actor abandoned the use of Firebase, and no longer tracked users using a dedicated URL. NOBELIUM's techniques shifted to encode the ISO within the HTML document and have that responsible for storing target host details on a remote server. The actor sometimes employed checks for specific internal Active Directory domains that would terminate execution of the malicious process if it identified an unintended environment.

#### **Indicators of Compromise**

Indicators of Compromise have been entered into Health-ISAC's automated sharing platform for those members ingesting automated threat indicators.

**Tactic-Techniques** 

Initial Access - Spearphishing Link, Command And Control - Application Layer Protocol, Execution - Malicious Link, Initial Access - Spearphishing via Service, Execution - Software Deployment Tools

#### Recommendations

- Turn cloud-delivered protection in Microsoft Defender Antivirus or the equivalent for your antivirus product to cover rapidly evolving attacker tools and techniques. Cloud-based machine learning protections block a huge majority of new and unknown variants.
- Run <u>EDR in block mode</u> so that Microsoft Defender for Endpoint can block malicious artifacts, even when your non-Microsoft antivirus doesn't detect the threat or when Microsoft Defender Antivirus is running in passive mode. (EDR in block mode works behind the scenes to remediate malicious artifacts that are detected post-breach.)
- Enable <u>network protection</u> to prevent applications or users from accessing malicious domains and other malicious content on the internet.
- Enable <u>investigation and remediation</u> in full automated mode to allow Microsoft Defender for Endpoint to take immediate action on alerts to resolve breaches, significantly reducing alert volume.
- Use <u>device discovery</u> to increase your visibility into your network by finding unmanaged devices on your network and onboarding them to Microsoft Defender for Endpoint.
- Enable multifactor authentication (MFA) to mitigate compromised credentials. Microsoft strongly encourages all customers download and use passwordless solutions like Microsoft Authenticator to secure your accounts.
- For Office 365 users, multifactor authentication support.
- For Consumer and Personal email accounts, see how to twostep verification.
- Turn on the attack surface reduction rule to block or audit activity associated with this threat: Block all Office applications from creating child processes. NOTE: <u>Assess rule</u> <u>impact</u> before deployment.

#### Sources

New sophisticated email-based attack from NOBELIUM

Microsoft Security Response Center

### Alert ID 5ceb8c8b

## **View Alert**

## Tags NOBELIUM

**TLP:WHITE** Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.





For more update and alerts, visit: <a href="https://health-isac.cyware.com">https://health-isac.cyware.com</a>

If you are not supposed to receive this email, please contact us at **toc@h-isac.org**.