


[Community \(https://community.infoblox.com/\)](https://community.infoblox.com/) | [Blog \(/\)](#) | [Cloud Services Login](#) | [Contact \(https://www.infoblox.com/contact-infoblox/\)](https://www.infoblox.com/contact-infoblox/) | 

[Why Infoblox \(https://www.infoblox.com/company/why-infoblox/\)](https://www.infoblox.com/company/why-infoblox/)

[Products \(https://www.infoblox.com/products/\)](https://www.infoblox.com/products/)

[Solutions \(https://www.infoblox.com/solutions/\)](https://www.infoblox.com/solutions/)

[Support & Services \(https://www.infoblox.com/support/\)](https://www.infoblox.com/support/)

[Resources \(https://www.infoblox.com/resources/\)](https://www.infoblox.com/resources/)

[Company \(https://www.infoblox.com/company/\)](https://www.infoblox.com/company/)

[Downloads \(https://www.infoblox.com/infoblox-download-center/\)](https://www.infoblox.com/infoblox-download-center/)

[Company \(https://blogs.infoblox.com/category/company/\)](https://blogs.infoblox.com/category/company/)

[Security \(https://blogs.infoblox.com/category/security/\)](https://blogs.infoblox.com/category/security/)

[Community \(https://blogs.infoblox.com/category/community/\)](https://blogs.infoblox.com/category/community/)

[IPv6 CoE \(https://blogs.infoblox.com/category/ipv6-coe/\)](https://blogs.infoblox.com/category/ipv6-coe/)

**[Cyber Threat Intelligence \(https://blogs.infoblox.com/category/cyber-threat-intelligence/\)](https://blogs.infoblox.com/category/cyber-threat-intelligence/)**

[Home \(https://blogs.infoblox.com/\)](https://blogs.infoblox.com/) / [Cyber Threat Intelligence](#)

[\(https://blogs.infoblox.com/category/cyber-threat-intelligence/\)](https://blogs.infoblox.com/category/cyber-threat-intelligence/) / [Cyber Campaign Briefs](#)

[\(https://blogs.infoblox.com/category/cyber-threat-intelligence/cyber-campaign-briefs/\)](https://blogs.infoblox.com/category/cyber-threat-intelligence/cyber-campaign-briefs/) /

Ukraine-Themed Malspam Drops Agent Tesla

**BRIEF**



# Ukraine-Themed Malspam Drops Agent Tesla



March 4, 2022

^

**Author: Christopher Kim**

## 1. Overview

On 1 March, Infoblox observed a malspam campaign that was using messages related to Russia's invasion of Ukraine. The malspam campaign was trying to lure users into downloading a ZIP file attachment whose contents could download the Agent Tesla keylogger.

This campaign occurred a week after Russia invaded Ukraine. It is one of multiple campaigns that have taken advantage of the conflict by luring users via socially engineered emails and websites with lookalike domains that serve fake donation content.<sup>1</sup>

## 2. Customer impact

Agent Tesla is a malware-as-a-service (MaaS) remote access trojan (RAT) that security researchers first discovered in 2014. It is usually distributed via spam or phishing emails, and it has many capabilities for stealing information from a victim's machine, including the following:

- logging keystrokes
- extracting data from the host's clipboard
- capturing screens
- grabbing forms
- stealing credentials from VPN software

After gathering sensitive information from a victim's machine, Agent Tesla exfiltrates the stolen information by using a web browser or an email client.

## 3. Campaign analysis

In this campaign, the threat actor(s) crafted messages using the email address supawadee.so@univance[.]co[.]th to impersonate UNIVANCE (Thailand) Co., Ltd: a manufacturer of automobile parts. The subject line is REQ : Supplier Survey : Effect of supply chain from the Ukraine/Russia conflict, and the body section is empty. The ZIP file attachment is named REQ Supplier Survey.zip and contains an embedded Microsoft Windows executable.

## 4. Attack chain

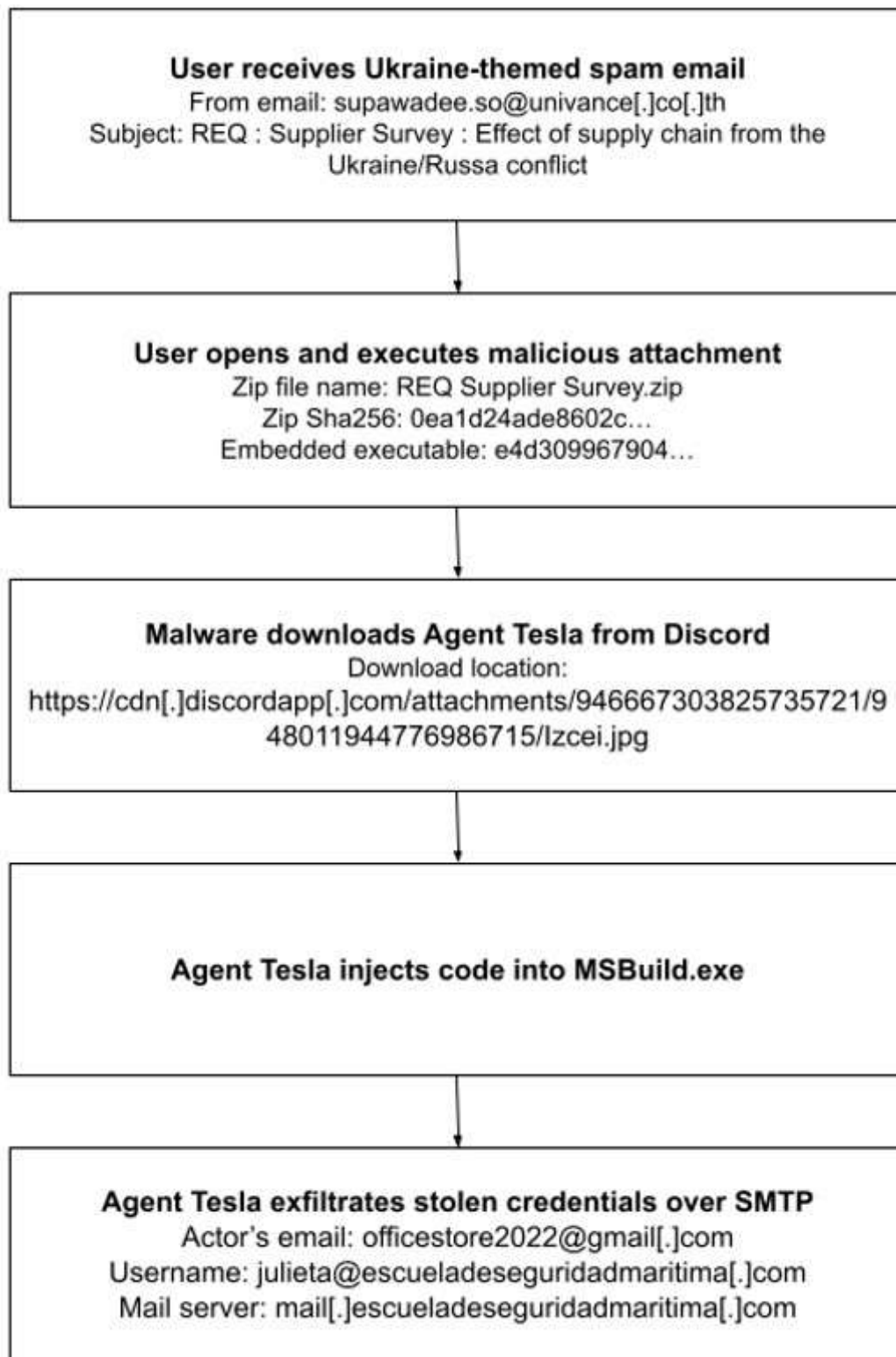
When a user extracts the ZIP file attachment, the embedded Windows executable is launched and writes itself to C:\Users\User\AppData\Roaming\Fgefvp\Gzgrfb.exe. A Run registry key is also created, and will enable Gzgrfb.exe to run every time the user signs in to the machine. Next, the malware downloads the Agent Tesla binary from

^

Discord's content delivery network (CDN) servers and injects the malicious code into the legitimate Windows process MSBuild.exe via process hollowing: a common technique for evading detection by antivirus software.<sup>2</sup>

Next, Agent Tesla steals account credentials and other sensitive information from the compromised system. It sends the stolen data to the actor's email account officestore2022@gmail[.]com via SMTP, by using the compromised email account julieta@escueladeseguridadmaritima[.]com and the email server mail[.]escueladeseguridadmaritima[.]com.





## 5. Vulnerabilities and mitigation

Agent Tesla is a dangerous RAT that can have severe and negative impact on its victims. Infoblox strongly recommends that businesses consider the following security measures:

- Be wary of opening emails from unfamiliar senders, and inspect unexpected attachments before opening them.
- Agent Tesla can also communicate with its C&C using a Tor client. Forbid the use of the Tor network if it is not crucial to business operations.
- Identify and flag API requests to messaging and CDN services, such as Discord. Such requests are indicative of unusual user behavior.
- Do not allow web browsers to save credentials or other sensitive information.

## Endnotes

1. <https://blogs.infoblox.com/cyber-threat-intelligence/cyber-threat-advisory/cyber-threat-advisory-ukrainian-support-fraud/>  
(<https://blogs.infoblox.com/cyber-threat-intelligence/cyber-threat-advisory/cyber-threat-advisory-ukrainian-support-fraud/>)
2. <https://attack.mitre.org/techniques/T1055/012/>  
(<https://attack.mitre.org/techniques/T1055/012/>)

**Appendix (downloadable list [here \(https://blogs.infoblox.com/wp-content/uploads/ukraine-themed-malspam-drops-agent-tesla.csv\)](https://blogs.infoblox.com/wp-content/uploads/ukraine-themed-malspam-drops-agent-tesla.csv))**

Representative Indicators of Compromise Description	Description
supawadee.so@univance[.]co[.]th	From email address
REQ : Supplier Survey : Effect of supply chain from the Ukraine/Russia conflict	Email subject
REQ Supplier Survey.zip	ZIP attachment file name
REQ Supplier Survey.exe	Executable file name
0ea1d24ade8602c0829bd73735ddfcdd6d6dfa12c6370e7cee0c04653a352839	ZIP file sha256
e4d309967904ca32fa5a00e70161c95621c687e46f2512bac1f061b0303fe863	Executable file sha256
hXXps://cdn[.]discordapp[.]com/attachments/946667303825735721/948011944776986715/lzcei[.]jpg	Agent Tesla download URL
officestore2022@gmail[.]com	Actor's email address
julieta@escueladeseguridadmaritima[.]com	Email address used for exfiltration
mail[.]escueladeseguridadmaritima[.]com	Email server used for exfiltration

+6

^

Labels: **Cyber Threat Intelligence** (<https://blogs.infoblox.com/tag/cyber-threat-intelligence/>)

**cyber security** (<https://blogs.infoblox.com/tag/cyber-security/>)

[malspam \(https://blogs.infoblox.com/tag/malspam/\)](https://blogs.infoblox.com/tag/malspam/)

[cyberthreat intelligence report \(https://blogs.infoblox.com/tag/cyberthreat-intelligence-report/\)](https://blogs.infoblox.com/tag/cyberthreat-intelligence-report/)

[Threat Intelligence \(https://blogs.infoblox.com/tag/threat-intelligence/\)](https://blogs.infoblox.com/tag/threat-intelligence/)



Infoblox Cyber Intelligence Group

With over 50 years of combined experience, the Infoblox Threat Intelligence Group creates, aggregates and curates information on threats to provide actionable intelligence that is high-quality, timely and reliable. Threat information from Infoblox filters out false positives and gives you the information you need to block the newest threats and to maintain a unified security policy across the entire security infrastructure of your organization.

[VIEW ALL POSTS \(/AUTHOR/CYBERINTEL-UNIT\)](#)

Products	Solutions	Company	Resources
DNS, DHCP & IPAM (DDI) (https://www.infoblox.com/products/ddi/)	Hybrid Workplace (https://www.infoblox.com/solutions/hybrid-workplace/)	About Us (https://www.infoblox.com/company/)	Resource Center (https://www.infoblox.com/resources/)
BloxOne® DDI (https://www.infoblox.com/products/bloxone-ddi/)	SaaS-Enabled Enterprise (https://www.infoblox.com/solutions/saas-enabled-enterprise/)	Why Infoblox (https://www.infoblox.com/company/why-infoblox/)	Support (https://www.infoblox.com/support/)
NIOS (https://www.infoblox.com/products/nios8/)	On-Premises + Cloud-Managed Networking (https://www.infoblox.com/solutions/on-premises-cloud-managed-networking/)	Platform Vision (https://www.infoblox.com/company/platform-vision/)	DNS Security Center (https://www.infoblox.com/dns-security-resource-center/)
BloxOne® Threat Defense (https://www.infoblox.com/products/bloxone-threat-defense/)		Market Leadership (https://www.infoblox.com/company/market-leadership/)	Infoblox Glossary (https://www.infoblox.com/glossary/)

bloxone-threat-defense/)	cloud-managed-networking/)	why-infoblox/market-leadership/)	Cyber Intelligence Unit
Advanced DNS Protection	Secure Services Edge	Customers	(https://infoblox.com/cyber-
(https://www.infoblox.com/products/advanced-dns-protection/)	(https://www.infoblox.com/solutions/secure-edge-services/)	(https://www.infoblox.com/company/customers/)	intelligence-unit/)
Cybersecurity Ecosystem	Networking Integrations	Infoblox Partner Programs	Community
(https://www.infoblox.com/products/cybersecurity-ecosystem/)	(https://www.infoblox.com/solutions/core-network-integrations/)	(https://www.infoblox.com/partners/)	(http://community.infoblox.com/)
Cloud Network Automation	Healthcare	Services	Training
(https://www.infoblox.com/products/cloud-network-automation/)	(https://www.infoblox.com/solutions/healthcare/)	(https://www.infoblox.com/support/)	(https://www.infoblox.com/support/training/)
Unified Network View	Higher Education	Press Releases	Blog (/)
(https://infoblox.com/products/network-insight/)	(https://www.infoblox.com/solutions/higher-education/)	(https://www.infoblox.com/company/press-releases/)	SaaS Status
IPAM for Microsoft	Public Sector	Careers	(https://status.infoblox.com/)
(https://infoblox.com/products/ipam-for-microsoft/)	(https://www.infoblox.com/solutions/public-sector/)	(https://www.infoblox.com/company/careers/)	Vulnerability Disclosure
	DevOps	Contact Us	(https://www.infoblox.com/vulnerability-responsible-disclosure-form)
	(https://www.infoblox.com/solutions/devops/)	(https://www.infoblox.com/company/contact/)	

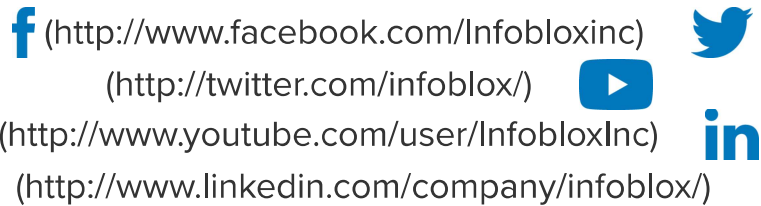
^



---

## Get Infoblox Email Updates

SUBSCRIBE



---

© 2022 Infoblox. All rights reserved. (<https://www.infoblox.com/>)

Feedback (<https://info.infoblox.com/feedback-form>)

Terms & Conditions (<https://www.infoblox.com/company/legal/website-terms-and-conditions/>)

Legal (<https://www.infoblox.com/legal/>)

Privacy Policy (<https://www.infoblox.com/company/privacy-policy/>)

Sitemap (<https://www.infoblox.com/sitemap/>)

