UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00145

RUST LANGUAGE GAINING TRACTION FOR MALWARE

DATE ISSUED: 24th May 2021

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	MEDIUM	**EASY**

OVERVIEW

A recent phishing campaign disguised as DHL shipping information or Microsoft communications has been distributing a new variant of the Buer malware written in the "easy-to-use" Rust programming language, enabling it to slip past a number of defences and avoid detection.

BREAKDOWN

The campaign has been dispersed containing two variants of the Buer malware – one in the common C programming language and the other in Rust – which may indicate that the purveyors are testing to see which is more effective at hooking victims and side-stepping security controls. Most commonly used as a first-stage downloader, Buer is used to gain a foothold in the compromised system and then install other malware such as a CobaltStrike beacon. It is also suspected that the next step could be to hire the new malware variant to other cybercriminals or sell systems infiltrated by RustBuer, as not all initial compromises resulted in the second-stage payload. The move to translate the malware to Rust could be to incorporate the greater features available with the Rust language, or may be potentially linked to Microsoft's new found interest in the language , joining the Rust Foundation in February

REMEDIATION STEPS

- Use SPAM and Secure Email Gateway filtering to prevent malicious emails from reaching your users.
- Use Next Generation Endpoint Protection Software on all user devices to detect and respond to suspicious activity that uses "time-of-click" protections.
- Use URL filtering to prevent access to known malicious sites.
- Educate users to raise awareness around social engineering and phishing emails and what to do within your organisation if they suspect an email is malicious.

REFERENCES & RESOURCES

Threatpost https://threatpost.com/buer-malware-loader-rewritten-rust/165782/
Proofpoint https://www.proofpoint.com/us/blog/threat-insight/new-variant-buer-loader-written-rust
ProSysCom https://www.prosyscom.tech/cyber-security/rust-buer-malware-variant-spotted/