

The Underground Economist: Volume 2, Issue 24

 zerofox.com/blog/the-underground-economist-volume-2-issue-24/

December 28, 2022



5 minute read

Welcome back to The Underground Economist: Volume 2, Issue 24, an intelligence focused blog series illuminating dark web findings in digestible tidbits from our [ZeroFox Dark Ops intelligence team](#). The Dark Ops team scours the dark web, extending visibility and engagement into places traditional security teams can't reach to share meaningful and insightful intelligence on the trends and tactics threat actors are leveraging across the dark web and criminal underground. Here's the latest for the week of December 23, 2022.

Rebranded Ransomware-As-A-Service Project Advertised

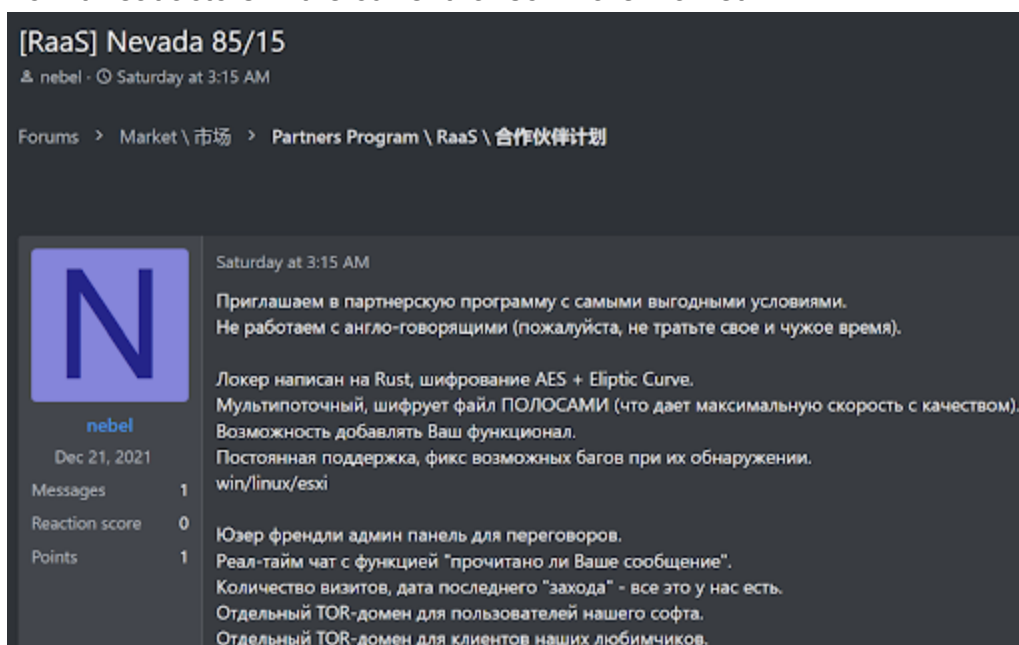
Untested threat actor "nebel" advertised what they claim is a new ransomware-as-a-service (RaaS) project, dubbed "Nevada," on the Russian language Dark Web forum "RAMP." Despite the actor's claims the project is new, ZeroFox researchers assess this is likely a rebranded version of an older RaaS project, dubbed "Luna," because the two have nearly identical features, including:

- Written in Rust

- Uses AES and ECC encryption
- Works on systems running Windows, Linux, and ESXI
- Controlled via administrator panel
- Contains real-time chat to negotiate with victims

Like the old project, the actor refuses to work with English-speaking threat actors. They also offered to split any successful ransom payments 85 to 15 in favor of affiliates, which is notable because most ransomware developers typically offer affiliates a smaller cut of the profits.

ZeroFox researchers assess the actor likely rebranded the initial “Luna” RaaS project because it failed to attract affiliates, indicating it is highly likely that there is a lull in interest from threat actors in the current ransomware market.



Original post from

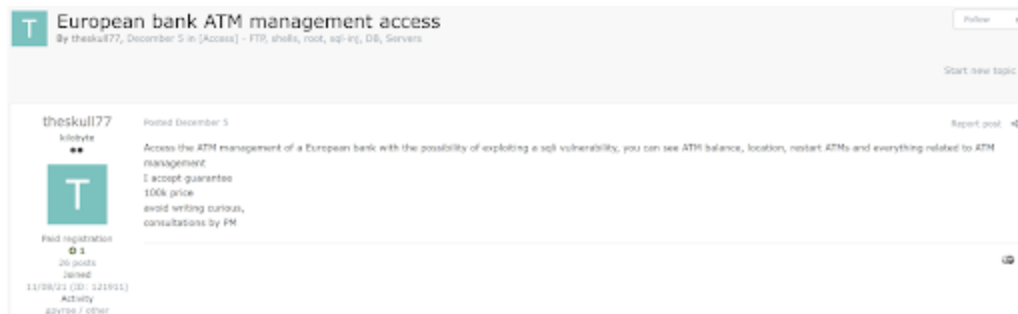
threat actor “nebel” advertising what they claim is a new ransomware-as-a-service (RaaS) project, dubbed “Nevada”

Actor Sells Access To ATM Management Software For Unnamed European Bank

In early December 2022, untested threat actor “theskull77” sold access to the ATM management software for an unnamed European bank on the predominantly Russian language forum “Exploit.” The alleged deal would allow threat actors to exploit a SQL injection vulnerability to steal sensitive data from the backend of the bank’s ATM network, including the balances and locations of various ATM machines. The actor said that operators can also restart the ATMs, which would likely allow a skilled threat actor to compromise the machines with malware and steal cash from the devices.

The asking price for the access started at \$100,000 USD, indicating the alleged buyer would likely expect to net a significant return on their investment.

ZeroFox researchers assess the actor is credible because they agreed to use the forum's escrow service, which would require them to deposit funds before a deal was brokered.



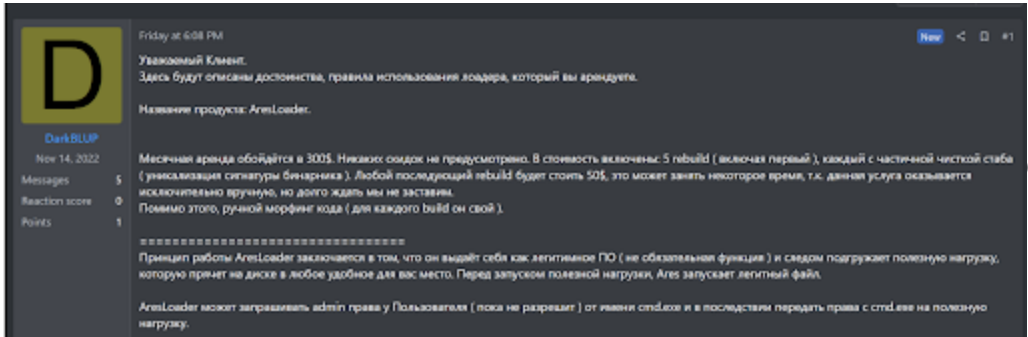
Threat Actors Abusing Malware Loader Developed As Penetration Testing Tool

New and untested threat actor “DarkBLUP” advertised a malware loader dubbed “Ares” on the Russian language Dark Web forum “RAMP.” ZeroFox researchers assess this loader is likely a legitimate penetration testing tool that is now being abused by threat actors. This is because of a similar project, dubbed “Project Ares,” was previously uploaded to GitHub as a proof-of-concept (PoC) by the well-regarded user and red teamer “CerberSec.”

The loader mimics legitimate software to trick victims into the executing malware with administrator rights on their machines.. Additional features of the loader include:

- Written in C/C++
- Supports 64-bit payloads
- Makes it look like malware spawned by another process
- Prevents non-Microsoft signed binaries from being injected into malware
- Hides suspicious imported Windows APIs
- Leverages anti-analysis techniques to avoid reverse engineering

The actor had ten licenses available for \$300 USD per month.



Original post from

threat actor “DarkBLUP” advertising a malware loader dubbed “Ares” on the predominantly Russian language Dark Web forum “RAMP”

Bundle Contains Exploits For Unpatched Vulnerabilities In Different Services

Well-regarded and established threat actor “LORD1” advertised a bundle containing exploits for unpatched vulnerabilities in different services, including Fortinet, Windows, Linux, Atlassian Bitbucket, VMware, and Oracle, on the predominantly Russian language Deep Web forum “Exploit.” The alleged exploits impact various remote code execution (RCE) vulnerabilities, tracked as:

- CVE-2022-40684 (Fortinet)
- CVE-2022-36804 (Atlassian Bitbucket)
- CVE-2021-39144, CVE-2022-31675, CVE-2022-22960 (VMware)
- CVE-2022-21497, CVE-2021-35587 (Oracle)

Additionally, the bundle contains exploits for several undisclosed local privilege escalation (LPE) vulnerabilities in Windows and Linux.

The actor charged \$4,000 USD for the bundle. They also had exploits for unpatched vulnerabilities in Veeam and Apache. The actor did not specify a price for these exploits.

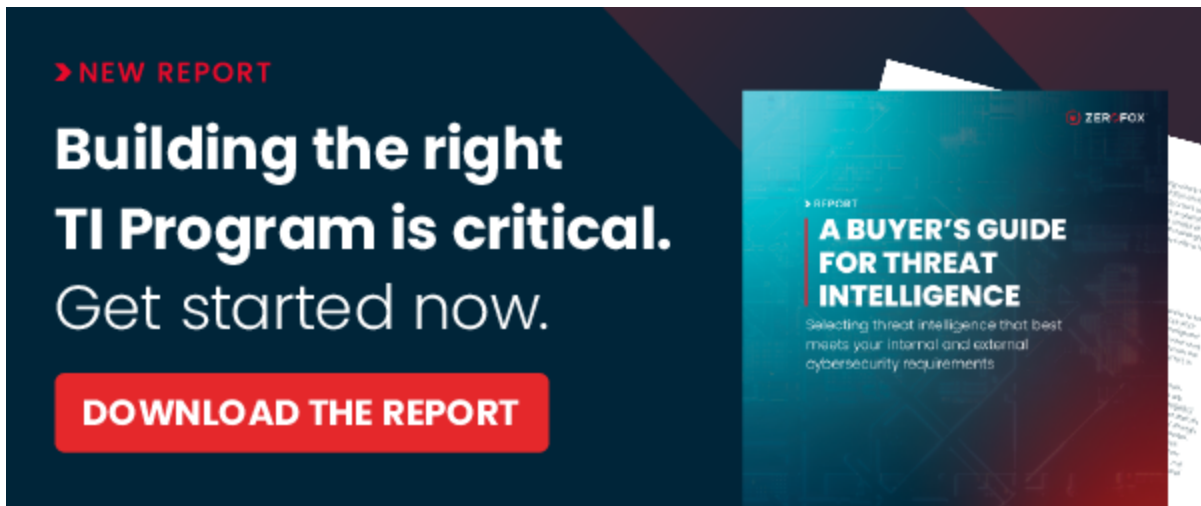
ZeroFox researchers assess the sale of this bundle would likely lower the barrier to entry for threat actors because the exploits come with an intuitive graphical user interface (GUI) and an integrated post-exploitation toolkit.



Original post from

threat actor “LORD1” advertising a bundle containing exploits for unpatched vulnerabilities in different services

For more insights and information on improving your threat intelligence strategy, download our Buyers Guide for Threat Intelligence.



> NEW REPORT

Building the right TI Program is critical. Get started now.

DOWNLOAD THE REPORT

ZEROFOX

REPORT

A BUYER'S GUIDE FOR THREAT INTELLIGENCE

Selecting threat intelligence that best
meets your internal and external
cybersecurity requirements

Tags: [Dark Ops](#) , [Deep & Dark Web](#) , [Threat Intelligence](#)