THREAT CURE

RE-ARCHITECT YOUR THREAT LANDSCAPE

ThreatCure

Cyber Threat Advisory

Lazarus Group

Threat Actor Malware

Description

Lazarus Group

CATEGORY

Malware

SEVERITY

High

Platforms

Windows & Linux

IMPACT

- Financial Theft
- Espionage
- Data Breaches
- Disruption of Services
- Reputational Damage

The Lazarus Group, also known as APT38, is a highly sophisticated hacking collective attributed to North Korea. Renowned for its advanced cyber espionage capabilities and financially motivated attacks, the group employs a range of tactics including malware deployment, spear-phishing, and exploiting vulnerabilities to compromise its targets. Its operations are supported by state resources, making its attacks particularly effective and damaging. Common indicators of its attacks include the use of trojans and ransomware, spear-phishing emails, deployment of custom malware, and communications with Command and Control (C2) servers.

Recently, the Lazarus Group has been linked to a series of ransomware attacks targeting major manufacturers in the United States and Europe. These campaigns aim to disrupt supply chains and extract ransom payments. Emerging trends suggest that the group is increasingly focusing on financially motivated attacks, with recent activities involving crypto currency exchanges and venture capital firms. This shift highlights the group's evolving tactics and its growing emphasis on financial gain.

Indicator of compromise

SHA-256

c9a7b42c7b29ca948160f95f017e9e9ae781f3b981ecf6edbac943e52c63ffc8
c7f4aa77be7f7afe9d0665d3e705dbf7794bc479bb9c44488c7bf4169f8d14fe
2360a69e5fd7217e977123c81d3dbb60bf4763a9dae6949bc1900234f7762df1
689cfaa9319f3f7529a31472ecf6b2e0ca6891b736de009e0b6c2ebac958cc94
c6a48365c3db9761bd60981bdcdd87aced23d8e60067caa30fee501bf4b47b84
a03d13c9825e150810e6e6aaf053d71ec5a53b86581414dd982a74d4a8bc5475
927b3564c1cf884d2a05e1d7bd24362ce8563a1e9b85be776190ab7f8af192f6
e6bbc33815b9f20b0cf832d7401dd893fbc467c800728b5891336706da0dbcec
a64fa9f1c76457ecc58402142a8728ce34ccba378c17318b3340083eeb7acc67
479038eb12ed07893ee0dcc04fbdcf182489bbb271f5a4f90f83874881a80ce3
2546d239a262c24a6f8ea01d890cbc459a22db79b379b6ec3b24fbb56efb5381
5009c7d1590c1f8c05827122172583ddf924c53b55a46826abf66da46725505a
87c5d0c93b80acf61d24e7aaf0faae231ab507ca45483ad3d441b5d1acebc43c
99dbc6fe3c3e465052fcefa1642861747dc9e069eeb244589b605bd710b1e0d1
fee4f9dabc094df24d83ec1a8c4e4ff573e5d9973caa676f58086c99561382d7
7667d1b8fcc4f712084e3e3f8b4ab505ab150c52aea7b219249ec508b4b0e224
6c121f2b2efa6592c2c22b29218157ec9e63f385e7a1d7425857d603ddef8c59
8bfa4fe0534c0062393b6a2597c3491f7df3bf2eabfe06544c53bdf1f38db6d4

081804b491c70bfa63ecdbe9fd4618d3570706ad8b71dba13e234069648e5e48
f3b0da965a4050ab00fce727bb31e0f889a9c05d68d777a8068cfc15a71d3703
5c907b722c53a5be256dc5f96b755bc9e0b032cc30973a52d984d4174bace456
5e40d106977017b1ed235419b1e59ff090e1f43ac57da1bb5d80d66ae53b1df8
973f7939ea03fd2c9663dafc21bb968f56ed1b9a56b0284acf73c3ee141c053c
0b5db31e47b0dccfdec46e74c0e70c6a1684768dbacc9eacbb4fd2ef851994c7
3c8dbfcbb4fccbaf924f9a650a04cb4715f4a58d51ef49cc75bfcef0ac258a3e
bce1eb513aaac344b5b8f7a9ba9c9e36fc89926d327ee5cc095fb4a895a12f80
bfd74b4a1b413fa785a49ca4a9c0594441a3e01983fc7f86125376fdbd4acf6b
cbf4cfa2d3c3fb04fe349161e051a8cf9b6a29f8af0c3d93db953e5b5dc39c86
91eaf215be336eae983d069de16630cc3580e222c427f785e0da312d0692d0fd
c83c7b000a955f2b8cb92bb112ed606ffd9fbebbe3422f80d90d06b167f2f37b
492a643bd1efdaca4ca125ade1b606e7bbf00e995ac9115ac84d1c4c59cb66dd
63fb47c3b4693409ebadf8a5179141af5cf45a46d1e98e5f763ca0d7d64fb17c
db6a9934570fa98a93a979e7e0e218e0c9710e5a787b18c6948f2eedd9338984
d8565d58ad8e4f5558b5cd70df0ad12be9cf44e32ad07aaac6f65b816edbf414
15d53bb839e00405a34a8b690ec181f5555fc4f891b8248ae7fa72bad28315a9
f1713afaf5958bdf3e975ebbab8245a98a84e03f8ce52175ef1568de208116e0

SHA-1

8d06e33097cd92876b3508117ce054cab76ad131

0ca239701ab8914d02345bdedf858ff88d5b54fd

2ae2d83c5bd27ef46fd08afaf6f018ba052debbc

0120251218b148c6446f7fc06cff5fa4c19027fd

1f284bfa302441c1c8a2c37935939eb998b7b2da

0ca239701ab8914d02345bdedf858ff88d5b54fd

0df3f5653584e0ddf0cff5b24106bf3c6cf30de9

1f6e13eeb7dfa22a12a38f8d2f1b927849b1db0a

06cdbeb58a4a1b93a7c7bd6d0dcf2a4fe0e23c66

31c3f71e53191c9f6f63aef2087f226b486d527b

MD-5

10a3aeedf4de7491648777444a0683e3

0d091e6683405901efe8df6d0da5b639

25fd301f06f7910ecde8861668cf5a21

0d091e6683405901efe8df6d0da5b639

4db7239eeb961ca764b82fcd0c4a7ab5

80f8ac5e48fdf233522c02e463fab9a7

ae6efca75c9555705ff9d69d1f6f67fe

0d091e6683405901efe8df6d0da5b639

0ddf3aa9d6e917729e1852b52546d4ae

1e3421f2395071e890eaa3267851e34b

Remediation

- Detection & Isolation: Use EDR/SIEM tools to detect malware and isolate affected systems.
- Malware Removal: Run antivirus scans, remove persistence mechanisms, and conduct deep system scans.
- Network Security: Strengthen firewall/IDS, segment critical systems, and monitor traffic.
- Access Controls: Enforce MFA, limit admin access, and reset compromised credentials.
- Recovery: Restore from clean backups, perform forensic analysis, and update incident response plans.
- Training: Conduct regular security training and phishing simulations.
- External Support: Engage third-party experts and report to authorities.
- Block all IOCs on your XDR, EDR and other security tools.

THREAT CURE
RE-ARCHITECT YOUR THREAT LANDSCAPE

ThreatCure

Cyber Threat Advisory

Secure your byte world

Lazarus Group

Threat Actor Malware

https://threatcure.net/

info@threatcure.net

+1 (832) 271 2738