Hive Pro

Threat Level

Red

THREAT ADVISORY

ATTACK REPORT

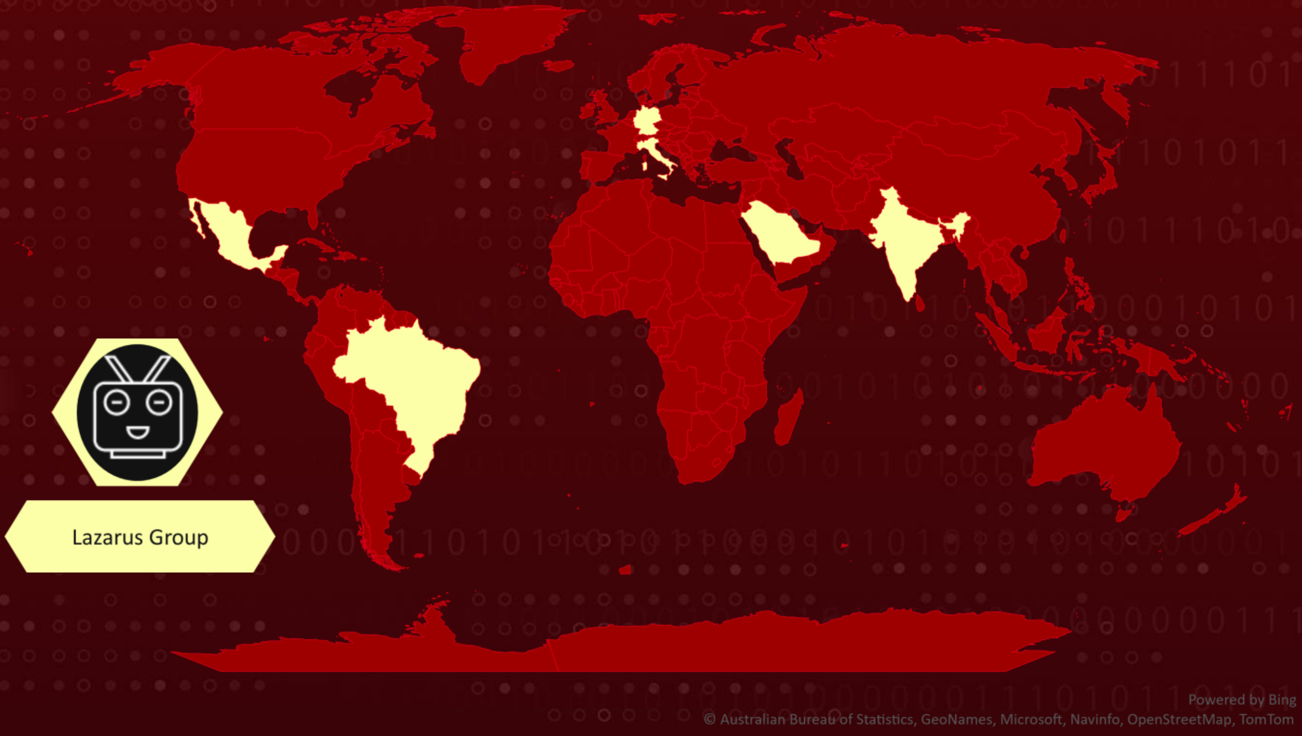
The DTrack Backdoor campaigns aimed European organizations

Date of Publication	Admiralty Code	TA Number
November 16, 2022	A1	TA2022259

Summary

First Activity Observed: 2019
Attack Region: Germany, Brazil, India, Italy, Mexico, Switzerland, Saudi Arabia, Turkey, and the United States.
Targeted Industry: Education, chemical manufacturing, governmental research centers, IT service providers, utility providers, and telecommunications.
Threat Actor: Lazarus Group
Attack: Backdoor masquerades as a genuine program, and there are multiple stages of decryption before the Final payload initiates.

Attack Regions


Lazarus Group
Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Attack Details

#1

DTrack, a malware developed by the Lazarus group is a flexible backdoor that unloads malware in stages. It is dispersed with filenames that are routinely used in legitimate executables. The backdoor is currently installed by infiltrating networks with stolen credentials or abusing Internet-exposed servers.

#2

DTrack decompresses the malware in phases. The malware's Portable Executable (PE) file contains the second stage. After obtaining the location and key for the next phase, the virus decrypts the buffer before loading its final payload via a process hollowing into an "explorer.exe" process that runs directly from memory.

#3

The libraries to be loaded in prior DTrack samples were obfuscated strings. In more recent versions, API hashing is utilized to load the appropriate libraries and functions.

Recommendations

Security Leaders
Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5’s Breach & Attack Simulation.

- **All Engineers:** Refer to and action upon the ’Potential MITRE ATT&CK TTPs’ & ‘Indicators of Compromise (IoC)’ on the following pages.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0009 Collection
TA0011 Command and Control	T1078 Valid Accounts	T1059 Command and Scripting Interpreter	T1059.003 Windows Command Shell
T1129 Shared Modules	T1547 Boot or Logon Autostart Execution	T1543 Create or Modify System Process	T1055 Process Injection
T1055.012 Process Hollowing	T1140 Deobfuscate/Decode Files or Information	T1056 Input Capture	T1056.001 Keylogging
T1083 File and Directory Discovery	T1082 System Information Discovery	T1560 Archive Collected Data	T1105 Ingress Tool Transfer

Indicator of Compromise (IOC)

TYPE	VALUE
MD5	1A74C8D8B74CA2411C1D3D22373A6769 67F4DAD1A94ED8A47283C2C0C05A7594
Domains	pinkgoat[.]com purewatertokyo[.]com purplebear[.]com salmonrabbit[.]com
IP Addresses	64.190.63[.]111 58.158.177[.]102 52.128.23[.]153 58.158.177[.]102

References

https://securelist.com/dtrack-targeting-europe-latin-america/107798/

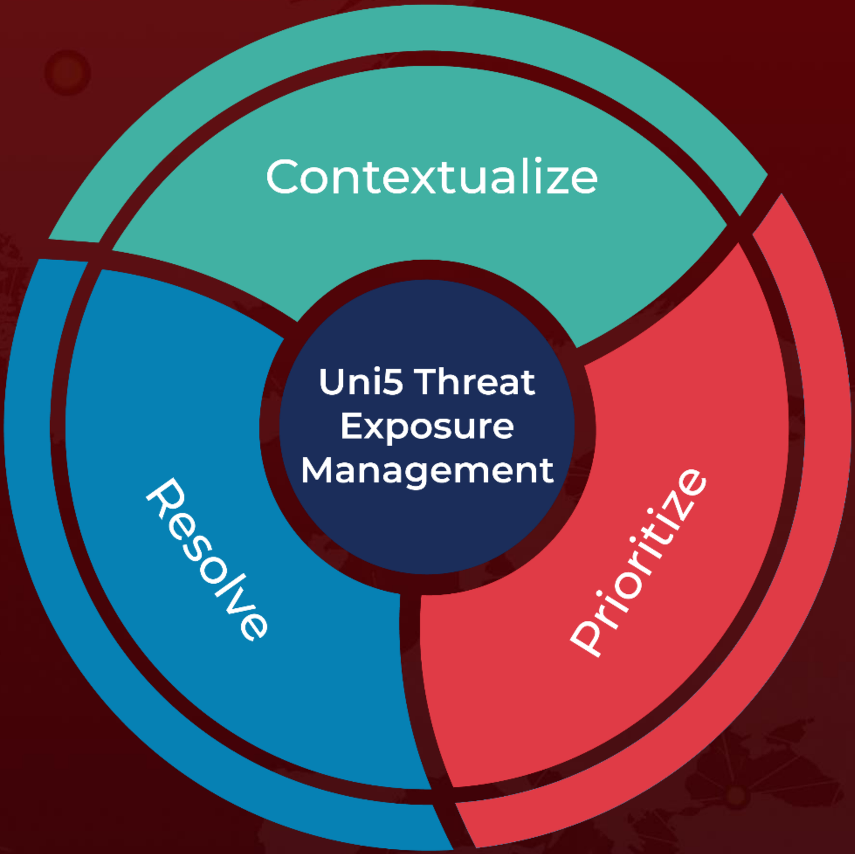
https://attack.mitre.org/software/S0567/

https://securelist.com/my-name-is-dtrack/93338/

What Next?

At **HivePro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **Hive Pro Uni5**: Continuous Threat Exposure Management Platform.



REPORT GENERATED ON

November 16, 2022 • 4:06 AM

More at www.hivepro.com