Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

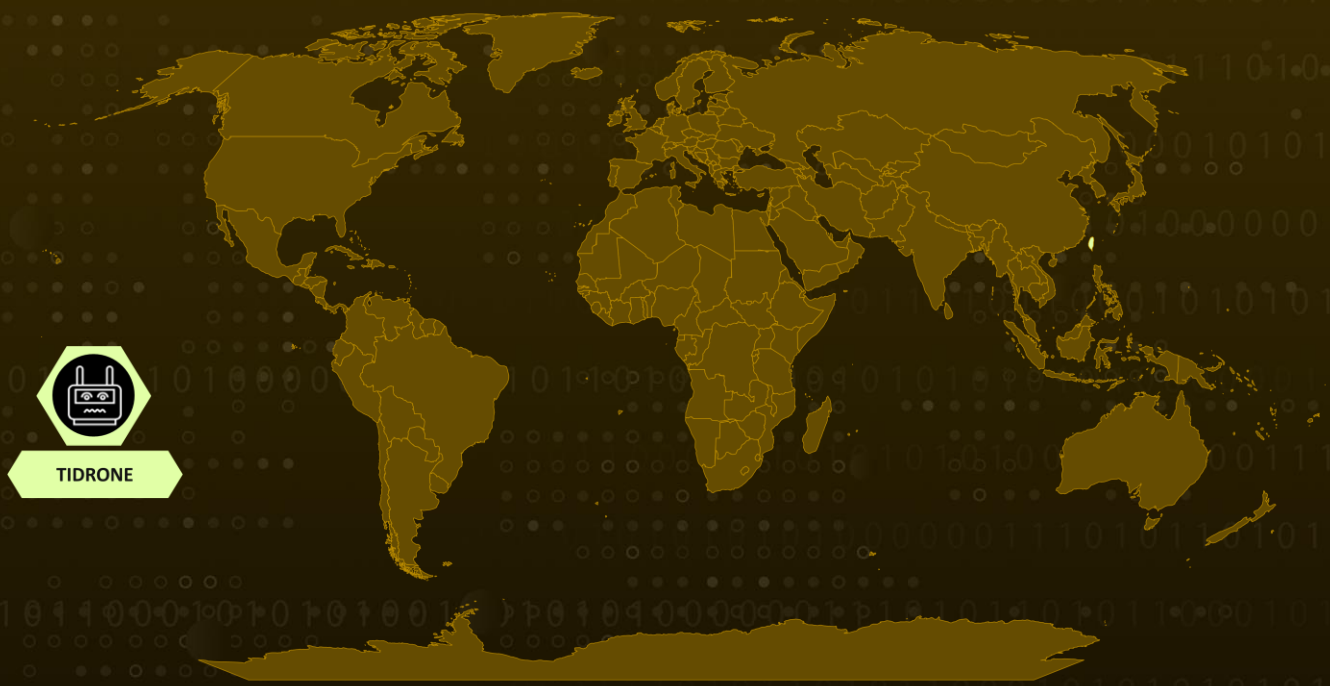
TIDRONE's Full-Scale Attack on Taiwan's Defense Industry

Date of Publication	Admiralty Code	TA Number
September 10, 2024	A1	TA2024347

Summary

Attack Began: 2024
Threat Actor: TIDRONE
Malware: CXCLNT, CLNTEND
Targeted Country: Taiwan
Targeted Industries: Military, Satellite, Drone Manufacturing Sector
Attack: TIDRONE, a Chinese-speaking threat actor, is actively targeting Taiwan's drone manufacturing and satellite industries, focusing on espionage and intelligence gathering. This sophisticated cyber espionage group deploys advanced malware, including CXCLNT and CLNTEND.

Attack Regions



Attack Details

#1 A Chinese-speaking threat group, dubbed TIDRONE, has demonstrated a keen focus on military-related supply chains, particularly targeting manufacturers in Taiwan's drone and satellite industries.

#2 This threat actor exploits enterprise resource planning (ERP) software and remote desktop protocols to deploy advanced malware toolsets, including CXCLNT and CLNTEND, with the primary aim of espionage and intelligence gathering.

#3 Evidence of exploited ERP systems in multiple victims' environments suggests that the malware is likely being spread through a supply chain attack, though the exact initial access vector remains unclear.

#4 The attack chain progresses through three distinct stages, designed to escalate privileges by bypassing User Account Control (UAC), harvesting credentials, and evading defenses by disabling antivirus software. Both backdoors are initiated through the sideloading of a malicious DLL file via Microsoft Word, enabling the attackers to exfiltrate sensitive data.

#5 CXCLNT acts as a backdoor, enabling communication between the compromised system and the command-and-control (C&C) server. It supports basic file upload and download capabilities, as well as features for erasing traces, gathering victim information, and downloading additional portable executable (PE) files for further execution.

#6 CLNTEND, delivered through a DLL named ClientEndPoint.dll, serves as a remote shell, providing attackers with full control over the infected system. It communicates with the C&C server using multiple protocols, including TCP, HTTP, HTTPS, TLS, and SMB (port 445).

Recommendations

Monitor and Control Remote Desktop Protocol (RDP) Usage: Disable unnecessary RDP services across the network to minimize potential attack vectors. Use multi-factor authentication (MFA) for RDP access to prevent unauthorized access in case of credential theft. Employ privileged access management (PAM) solutions to monitor and control administrative access over RDP connections.

Implement Traffic Monitoring: Monitor network traffic for suspicious activities, including outbound connections to unusual domains or IP addresses, particularly those involving TCP, HTTPS, SMB, and other protocols used by TIDRONE's malware.

Harden Systems Access Controls and Credential Security: Use credential guard technologies and regularly monitor for suspicious credential access or dumping activities. Rotate administrative credentials regularly and ensure that credentials are not reused across different systems or vendors.

Secure Common Entry Points: Use application control policies to only allow trusted and verified applications to execute, blocking potentially malicious payloads. Regularly scan email attachments and monitor for suspicious LNK and DLL files, which may be used for initial infection.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection
TA0011 Command and Control	TA0010 Exfiltration	T1203 Exploitation for Client Execution	T1574 Hijack Execution Flow
T1574.002 DLL Side-Loading	T1548 Abuse Elevation Control Mechanism	T1548.002 Bypass User Account Control	T1562 Impair Defenses
T1562.001 Disable or Modify Tools	T1036 Masquerading	T1036.005 Match Legitimate Name or Location	T1040 Network Sniffing
T1212 Exploitation for Credential Access	T1083 File and Directory Discovery	T1012 Query Registry	T1057 Process Discovery
T1119 Automated Collection	T1021.001 Remote Desktop Protocol	T1071.001 Web Protocols	T1041 Exfiltration Over C2 Channel

T1082 System Information Discovery	**T1070** Indicator Removal	**T1543** Create or Modify System Process	**T1055** Process Injection
T1560 Archive Collected Data	**T1071.002** File Transfer Protocols	**T1071** Application Layer Protocol	**T1021** Remote Services
T1105 Ingress Tool Transfer			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	8cfb55087fa8e4c1e7bcc580d767cf2c884c1b8c890ad240c1e7009810af6736, f13869390dda83d40960d4f8a6b438c5c4cd31b4d25def7726c2809ddc573dc7, e366f0209a939503418f2b7befbd60b79609b7298fed9c2fbafcb0e7fde19740, 6cb08a458e35101ef1035e7926130e1394cc1764a10166628aff541834c67063, 19bbc2daa05a0e932d72ecfa4e08282aa4a27becaabad03b8fc18bb85d37743a, eea0f94c6a8f18275c3dac1e1b9e9d3240e37073ff391852e8ff8d8391efa9aa, 0d91dfd16175658da35e12cafc4f8aa22129b42b7170898148ad516836a3344f, 1b08f1af849f34bd3eaf2c8a97100d1ac4d78ff4f1c82dbea9c618d2fcd7b4c8, 4b5f609c6b6788bdf0b900dd3df3c982cd547e7925840000bdc4014f8a980070, 1f22be2bbe1bfcda58ed6b29b573d417fa94f4e10be0636ab4c364520cda748e, 3b8f10a780eb64a3c59a2ae85fec074faf0f1a8d9725fb111f5cbf80e7b0dc1b, db600b0ae5f7bfc81518a6b83d0c5d73e1b230e7378aab70b4e98a32ab219a18, 1bf318c94fa7c3fb26d162d08628cef54157dfeb2b36cf7b264e3915d0c3a504, f3897381b9a4723b5f1f621632b1d83d889721535f544a6c0f5b83f6ea3e50b3

TYPE	VALUE
Domains	bestadll[.]fghytr[.]com, client[.]wns[.]windowswns[.]com, server[.]microsoftsvc[.]com, service[.]symantecsecuritycloud[.]com, time[.]vmwaresync[.]com

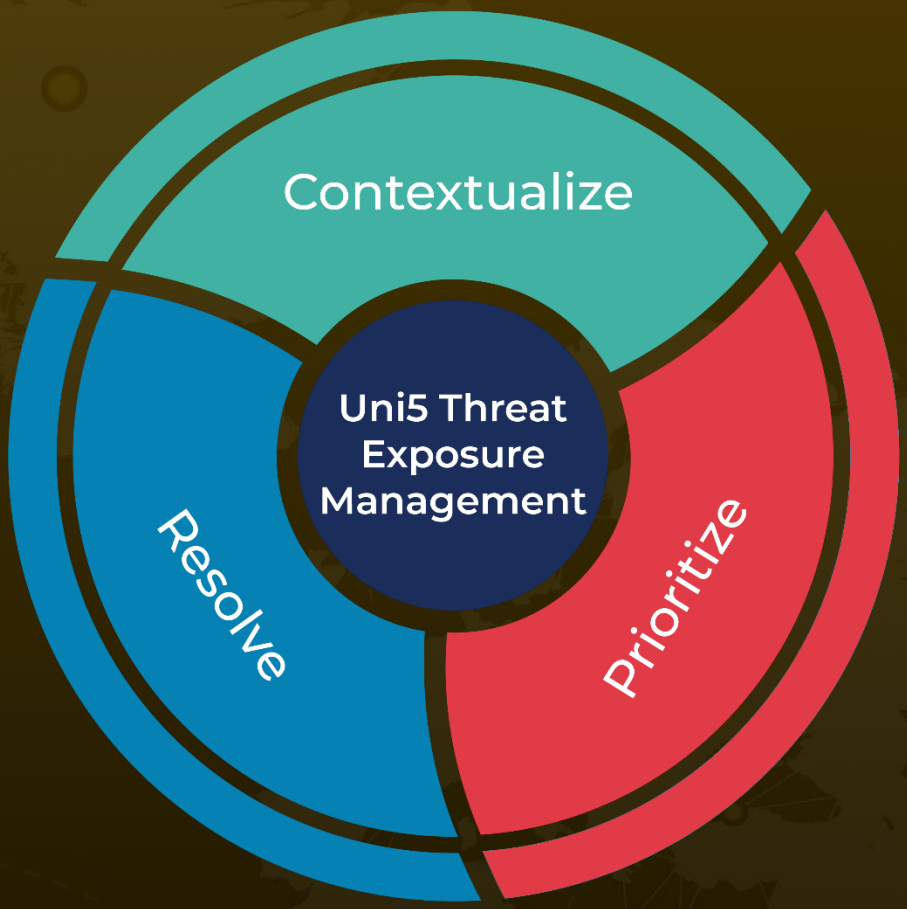
References

https://www.trendmicro.com/en_us/research/24/i/tidrone-targets-military-and-satellite-industries-in-taiwan.html

What Next?

At **Hive Pro**, 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 **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

September 10, 2024 • 6:30 AM

More at www.hivepro.com