Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ACTOR REPORT

Revealing the Tonto Team's Latest Hacks and Menaces

Date of Publication	Admiralty code	TA Number
February 14, 2023	A1	TA2023079

Summary

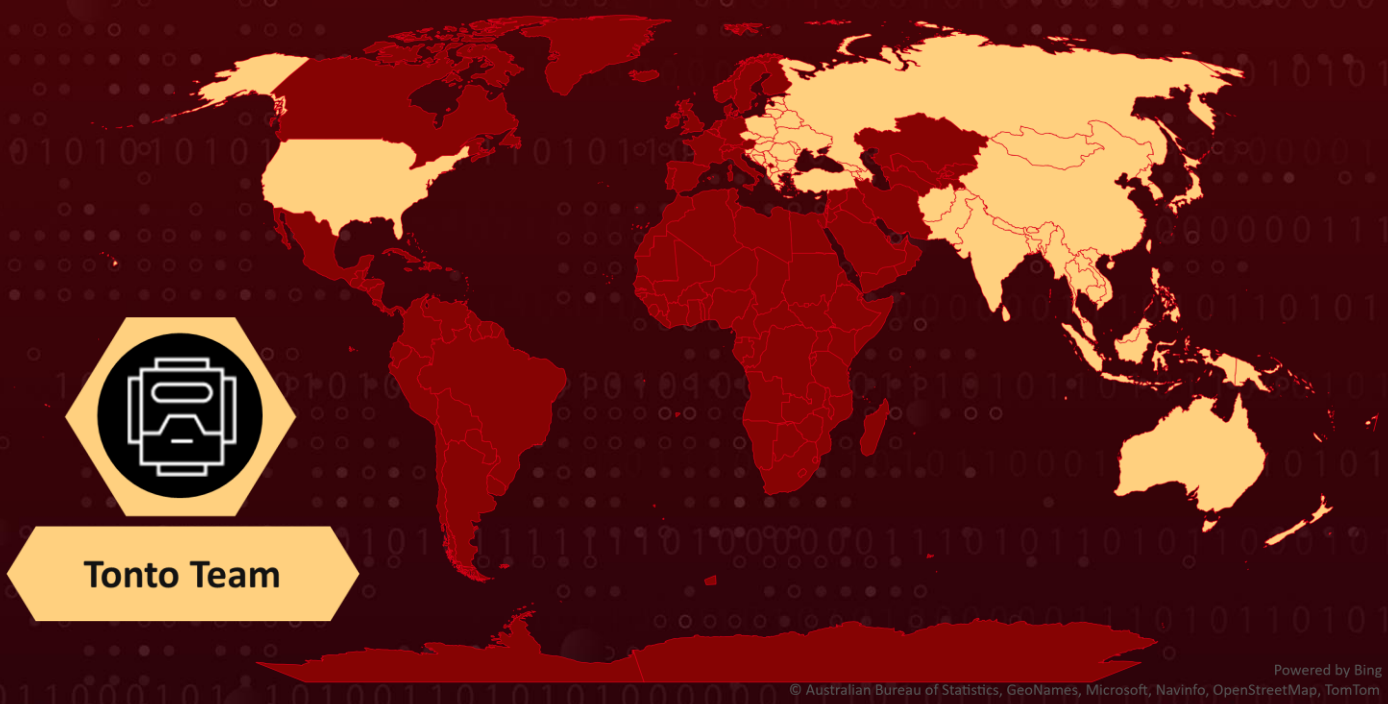
First Appearance: 2009
Actor Name: Tonto Team
Target Industries: Government, Defense, IT, Energy, Financial, Educational, Healthcare, Media, and Technology
Target Region: India, Japan, Mongolia, Russia, South Korea, Taiwan, USA, and Eastern Europe.

CVEs

CVE	NAME	PATCH
CVE-2017-11882	Microsoft Office Memory Corruption Vulnerability	✓
CVE-2018-0802*	Microsoft Office Memory Corruption Vulnerability	✓
CVE-2018-0798	Microsoft Office Memory Corruption Vulnerability	✓

*zero-day vulnerability

Actor Map



Actor Details

#1

The Tonto Team threat actors pretended to be employees of a reputable organization and utilized a GMX Mail-created phony email. The enclosed file is a malicious Rich Text Format (RTF) document developed with the Royal Road RTF Weaponizer. Chinese APT organizations are the primary users of the weaponizer. The tool enables the threat actor to construct malicious RTF exploits with realistic decoy content for the Microsoft Equation Editor vulnerabilities CVE-2017-11882, CVE-2018-0802, and CVE-2018-0798.

#2

The decrypted payload was a Bisonal-classified malicious EXE file in PE32 format. Backdoor for a DoubleT. This malware lets an attacker to get remote access to an infected computer and run various instructions on it in order to gather information about the compromised host. The hacked host's information is encoded using the Base32 method. The data sent in a POST request is encrypted using the same RC4 method in a non-standard 128-byte implementation.

#3

The primary objectives of Chinese APTs are espionage and intellectual property theft. Undoubtedly, the Tonto Team will continue to probe IT and cybersecurity firms by utilizing spear phishing to transmit infected documents using vulnerabilities and decoys expressly created for this purpose.

Actor Group

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGET REGIONS</th><th>TARGET INDUSTRIES</th></tr>
<tr><td rowspan="3">Tonto Team (HeartBeat, Karma Panda, CactusPete, Bronze Huntley, LoneRanger, Earth Akhlut)</td><td>China</td><td rowspan="3">India, Japan, Mongolia, Russia, South Korea, Taiwan, USA, and Eastern Europe</td><td rowspan="3">Government, Defense, IT, Energy, Financial, Educational, Healthcare, Media, and Technology</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td></tr>
</table>

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 actor 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	TA0008 Lateral Movement
TA0009 Collection	TA0011 Command and Control	TA0010 Exfiltration	TA0040 Impact
T1566 Phishing	T1566.001 Spearphishing Attachment	T1204 User Execution	T1204.002 Malicious File
T1203 Exploitation for Client Execution	T1059 Command and Scripting Interpreter	T1059.003 Windows Command Shell	T1547 Boot or Logon Autostart Execution
T1547.001 Registry Run Keys / Startup Folder	T1027 Obfuscated Files or Information	T1140 Deobfuscate/Decode Files or Information	T1056 Input Capture
T1124 System Time Discovery	T1057 Process Discovery	T1082 System Information Discovery	T1016 System Network Configuration Discovery
T1614 System Location Discovery	T1614.001 System Language Discovery	T1033 System Owner/User Discovery	T1210 Exploitation of Remote Services
T1071 Application Layer Protocol	T1071.001 Web Protocols	T1573 Encrypted Channel	T1573.002 Asymmetric Cryptography
T1001 Data Obfuscation	T1105 Ingress Tool Transfer	T1041 Exfiltration Over C2 Channel	T1491 Defacement

Indicator of Compromise (IOCs)

TYPE	VALUE
URLs	hxxp[:]//137.220.176[.]165/ru/order/index.php?strPageID=234989760 hxxp[:]//www.offices-update[.]com/ru/order/index.php?strPageID=234989760 hxxps[:]//upportteam[.]lingrevelat[.]com/update/v32/default
IP Addresses: Port	103.85.20[.]194:443 137.220.176[.]165:443 137.220.176[.]215
Domains	upportteam[.]lingrevelat[.]com supportteam[.]lingrevelat[.]com news[.]wooordhunts[.]com
Mutexes	A931568B-94AF-449D-B7F6-6585EF9E9839
MD5	80987dcdb36e7cb52bb03f00261aa2bd 67bfa75dbc39ab88da995c21565d05ca b8387fc571a8e79efab3e2cc343aae24 001b53acfab523dc060d38d73d63feef 518439fc23cb0b4d21c7fd39484376ff e40c514739768ba04ab17ff0126c1533 7c138c6b6f88643d7c16e741f98e0503 d5d0a1a034dcefdb08d9ca51c7694a22 40caac250ef2f2937521e4d8374477e7 f53965ab81f746f5a2bf183d2a704c72 8cdd56b2b4e1e901f7e728a984221d10 83b8d4462566a23298ca38c418eeccde 66c46b76bb1a1e7ecdb091619a8f5089 543bb103b8ad231ca53f6c1eb369c094 d748141a5878b7ef21c2663e9a1cdd2d d598baa47b9bcb4f5059a81515f9480b ab5cd5dfc157c70b9872fed13774e039
SHA1	071f19019fa7b8fae94aace54167c1b085f5c050 159b8b3bddbe60654d2be40416c6d6e74eeb86fa 1c848911e6439c14ecc98f2903fc1aea63479a9f 295a4c55c24260fad46e00f6935c7172f207c247 2abf70f69a289cc99adb5351444a1bd23fd97384 2b7975e6b1e9b72e9eb06989e5a8b1f6fd9ce027 415ce2db3957294d73fa832ed844940735120bae 5b01f3425b8fd053bd93b0d0aef2f04a950de7b2 5c22539218a08e9ec181cb2d89853b9aeb65c1bc 9d5daba847044ab63c926f9c740e47ee079f09d6

TYPE	VALUE
SHA1	a501fec38f4aca1a57393b6e39a52807a7f071a4 c9e4390ae500fc4d9704b665f981a61bc504bf46 cb8eb16d94fd9242baf90abd1ef1a5510edd2996 d858d9e11fc027ce7102ef150b412d1eaf34c544 dc943ff76af8384913bc0b79573fea71c7999a08 f599ed4ecb6c61ef2f2692d1a083e3bb040f95e6 f714f02e935bc70f3b10184b15343601b33a24d2
SHA256	0828b9834e1f967fc68d7dd577cc40c63715ee1a37786437c46af3ccd6ac79ea,0f704f3ab4a3ec30656dab6094c582b1089cbc8fcba280cadf3c7a651aeaacc3,10f881212a7c60f1da2f0b0473a7f1dd0af0b99a1e154f46f7fed45d92b7b05d,1c86452b222c8e631b0434585000466814f92f71d81576e03e0a118409019842,43622526694b40bad5fde8971f7937a22b8e6f4012dbd39cd4746429e056c609,58c1cab2a56ae9713b057626953f8967c3bacbf2cda68ce104bbb4ece4e35650,64fabaf342a23f1777f6895383eddb4fc065d6c4d8608cebea51c30064b5c2a8,7944fa9cbfef2c7d652f032edc159abeaa1fb4fd64143a8fe3b175095c4519f5,7970393e506934e9304f1d18ced34b86ef04a0d278d8e3cdb4b0064caee73846,8597e6b9f5f61c68a9ef219513dd43dd36e269b738f849b1dda44b576c865d39,bc78ba16d9495b17918d31e893a5f10d8a87d16a4a88f9bfd3ed5c735ce2ae11,c2ba362693aad8686f79822712c3871f0da1570465578843f5d73c70db07e631,c357faf78d6fb1460bfcd2741d1e99a9f19cf6dffd6c09bda84a2f0928015398,c7018ee3783f4b2fb19fedc78c59586390efa1b72c907867794bf42141eb767c,d79dcb90dfc01723f8df5628f502352c6f922187d3ef5942a6e8465552f40edf,dcb854e32d3ca08852371673ed7cd9139af761b8b127113746a527050b5e2b1d,f76f3277385195c27fdf2f90a01a8dd70bd05d92ab70696a6e6d7b0d5fb8e70c

Patch Links

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2017-11882

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2018-0802

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2018-0798

References

https://www.group-ib.com/blog/tonto-team/

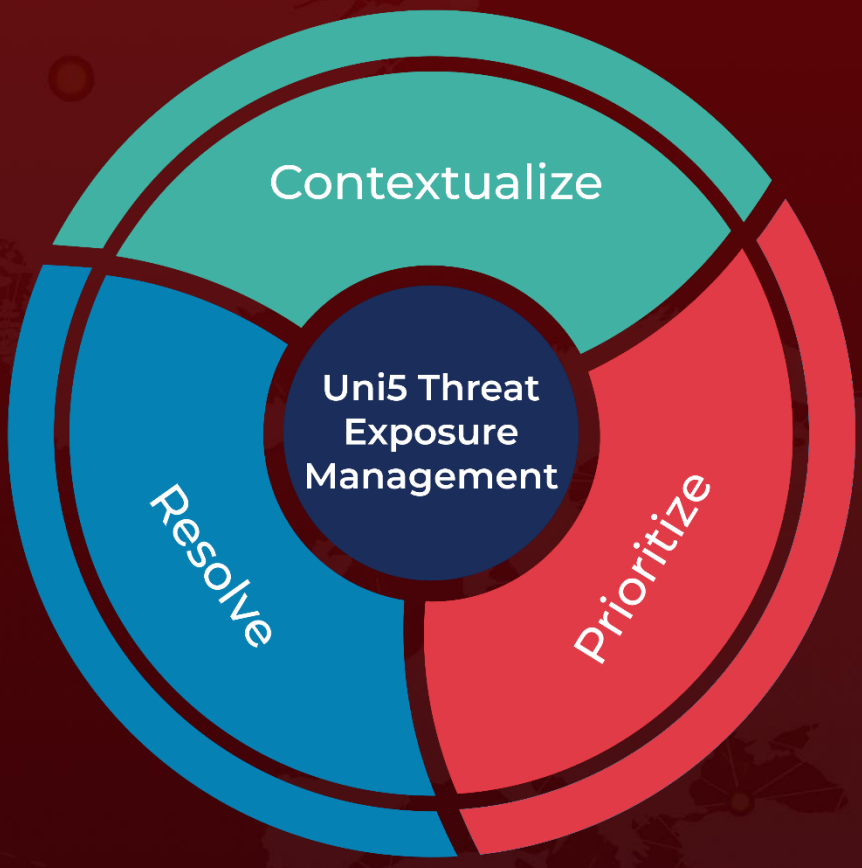
https://thehackernews.com/2023/02/chinese-tonto-team-hackers-second.html?&web_view=true

https://attack.mitre.org/groups/G0131/

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

February 14, 2023 . 4:44 AM

More at www.hivepro.com