Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ACTOR REPORT

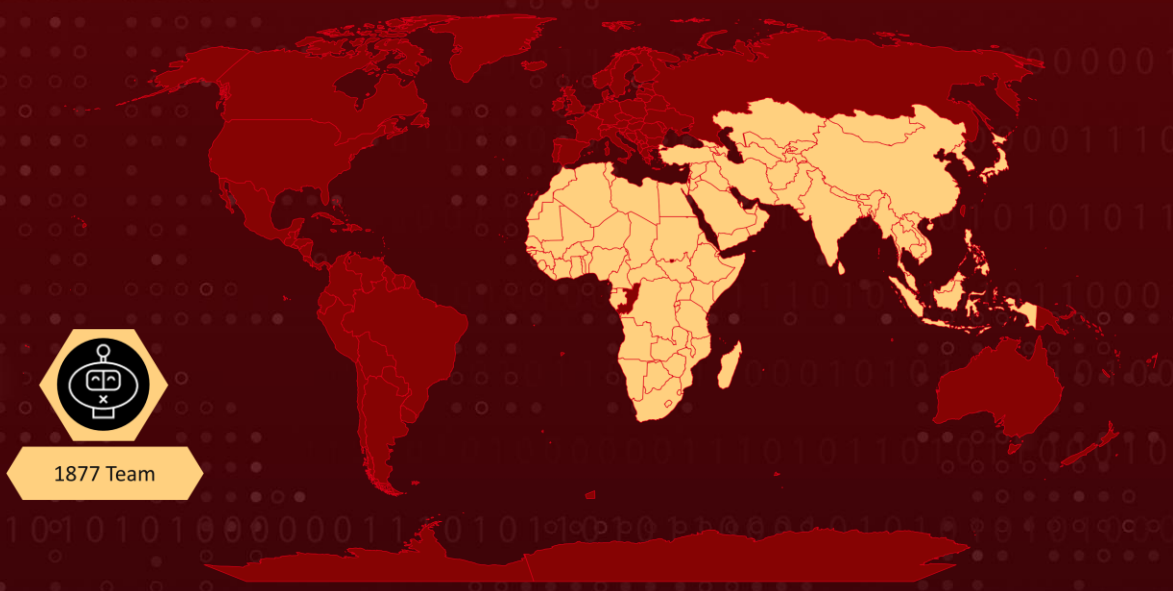
The Emergence of 1877 Team and Rising Hacktivist Threat

Date of Publication	Admiralty code	TA Number
May 4, 2023	A1	TA2023210

Summary

First Appearance: July 2021
Actor Name: 1877 Team
Target Regions: Middle East, Africa, Asia
Target Sectors: Governments, Universities, Telecommunication, Defense, and IT

Actor Map



Actor Details

#1 The 1877 Team is a hacktivist collective founded by a small group of Iraqi Kurds in July 2021. Their activities have become more sophisticated and politically driven, and they are now considered an emerging threat to a range of organizations. Their self-proclaimed goals include pressuring governments, spreading public dissent, and gaining notoriety amongst their fellow criminals.

#2 The 1877 Team has claimed responsibility for a range of cyber attacks on national governments, universities, telecommunication companies, defense organizations, and IT corporations. While their primary targets are in the Middle East, organizations in Africa, Asia, and the West have also been affected.

#3 The group operates a social media service, a defacement exposure website, and a dark web forum for trading exploits, malware, and stolen information. They have established close links with skilled hacktivist collectives such as Anonymous, AnonGhost, and ALtharea.

#4 The group employs two simple techniques to gain access to foreign infrastructure: scans of web pages for vulnerabilities and brute-forcing administrator credentials. Their attacks often involve website defacements, DDoS attacks, and leaks of sensitive information.

#5 Although the group's political affiliations and views appear volatile and at times contradictory, their activities are strongly influenced by their political affiliations. The 1877 Team appears to consist of around a dozen Iraqi-Kurdish teenagers/young adults, with the founder (alias: Overthinker1877) and co-founder (alias: CodeBoy1877) primarily carrying out their activities. The group has a significant social media following, with 12,000 members on their Telegram channel alone.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
1877 Team	Kurdistan **MOTIVE** Hacktivist	Middle East, Africa, Asia	Governments, Universities, Telecommunication, Defense, and IT

Recommendations

Use a firewall: You can use a firewall to block incoming traffic from the IP addresses. This will prevent any traffic from the specified IPs from reaching your network.

Monitor Dark Web Activity: Organizations should monitor the dark web for any mentions of their organization or information being traded. This can help identify potential threats and prevent data breaches.

Increase Cybersecurity Measures: Organizations should ensure they have robust cybersecurity measures in place, including regular vulnerability scanning and penetration testing. They should also implement multi-factor authentication and limit administrative access to prevent brute-forcing attacks.

Educate Employees: Organizations should educate their employees on cybersecurity best practices, including not clicking on suspicious links or downloading attachments from unknown sources. Additionally, they should have an incident response plan in place in case of a cyber attack.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0009 Collection	TA0011 Command and Control
TA0040 Impact	T1003 OS Credential Dumping	T1005 Data from Local System	T1010 Application Window Discovery
T1012 Query Registry	T1018 Remote System Discovery	T1027 Obfuscated Files or Information	T1027.002 Software Packing
T1033 System Owner/User Discovery	T1036 Masquerading	T1047 Windows Management Instrumentation	T1055 Process Injection
T1055.012 Process Hollowing	T1056 Input Capture	T1056.001 Keylogging	T1057 Process Discovery

T1059 Command and Scripting Interpreter	T1059.003 Windows Command Shell	T1070 Indicator Removal	T1070.006 Timestomp
T1071 Application Layer Protocol	T1082 System Information Discovery	T1083 File and Directory Discovery	T1087 Account Discovery
T1095 Non-Application Layer Protocol	T1105 Ingress Tool Transfer	T1112 Modify Registry	T1113 Screen Capture
T1115 Clipboard Data	T1119 Automated Collection	T1129 Shared Modules	T1134 Access Token Manipulation
T1213 Data from Information Repositories	T1219 Remote Access Software	T1222 File and Directory Permissions Modification	T1497 Virtualization/Sandbox Evasion
T1497.001 System Checks	T1518 Software Discovery	T1518.001 Security Software Discovery	T1529 System Shutdown/Reboot
T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder	T1547.004 Winlogon Helper DLL	T1562 Impair Defenses
T1562.001 Disable or Modify Tools	T1564 Hide Artifacts	T1564.003 Hidden Window	T1571 Non-Standard Port
T1614 System Location Discovery	T1614.001 System Language Discovery	T1620 Reflective Code Loading	

Indicator of Compromise (IOCs)

TYPE	VALUE
MD5	148264565031a8ebb6887a1395a2247a b3503746bb7f1d30755c9f4a26ce0a2c 99e19c4a4a8a972005902bf6129867e9
SHA256	334c23c94f9c6587e2afd0689796daa8791fda9b823b23836893b86f5cce849f 683fa1e449da9b71d0cafefb107efd97f0f8163f844dd837d12c354c2b901b93
IPV4	203.156.136[.]113 5.206.227[.]115 185.11.145[.]254

TYPE	VALUE
Domains	hawler.duckdns[.]org overthinker1877.duckdns[.]org 1877[.]to 1877[.]team 1877[.]krd zone.1877[.]team social.1877[.]team tube.1877[.]team shop.1877[.]team tools.1877[.]team 4567987654345265[.]tk asadohostma[.]cf asadohostma[.]tk balotelaras[.]gq bjigcdrfbbcx[.]ml bjigcdrfbbcx[.]tk bruthoosbxyxio[.]gq bsidbxiooohzu[.]ga bsidbxiooohzu[.]gq bsidbxiooohzu[.]ml buhgdkurd444[.]ga coalermallwive[.]ga forever0g[.]tk ghiiidueebsxiis[.]ml ghiiidueebsxiis[.]tk hsushzidooonsnx[.]gq htetryfugyioiyut[.]ml huncho[.]ml jfueytg7yghg[.]ga jihugkyfjtdsrytsrd[.]cf jihugkyfjtdsrytsrd[.]gq makolo[.]ml oiuryhgyefdter[.]gq salogo[.]gq steetdre6iazwed[.]tk stiwebbro[.]ml stupuviijvftuiu[.]cf tgfr43e98uj43ef[.]ml torontos[.]ga vanuboutst[.]cf vanuboutst[.]ml wpojgbjffy444[.]cf yjksvjdbjdbjjda[.]cf yjksvjdbjdbjjda[.]ga yjksvjdbjdbjjda[.]ml yjksvjdbjdbjjda[.]tk unconditional[.]gq

TYPE	VALUE
Websites	www.4567987654345265[.]tk www.asadohostma[.]cf www.asadohostma[.]tk www.balotelaras[.]gq www.bjigcdrfbbcx[.]ml www.bjigcdrfbbcx[.]tk www.bruthoosbxyxio[.]gq www.bruthoosbxyxio[.]tk www.bsidbxiooohzu[.]ga www.bsidbxiooohzu[.]gq www.buhgdkurd444[.]ga www.coalermallwive[.]ga www.forever0g[.]tk www.ghiiidueebsxiis[.]ml www.hawler.duckdns[.]org www.hsushzidooonsnx[.]gq www.htetryfugyioiyut[.]ml www.huncho[.]ml www.jagajaga[.]ga www.jfueytg7yghg[.]ga www.jihugkyfjtdsrytsrd[.]cf www.jihugkyfjtdsrytsrd[.]gq www.linkup[.]pics www.oiuryhgyefdter[.]gq www.salogo[.]gq www.steetdre6iazwed[.]tk www.stiwebbro[.]ml www.stupuviijvftuiu[.]cf www.tgfr43e98uj43ef[.]ml www.torontos[.]ga www.ukyudrst.zyns[.]com www.vanuboutst[.]cf www.wpojgbjffy444[.]cf www.yjksvjdbjdbjjda[.]cf www.yjksvjdbjdbjjda[.]ga www.yjksvjdbjdbjjda[.]ml www.yjksvjdbjdbjjda[.]tk

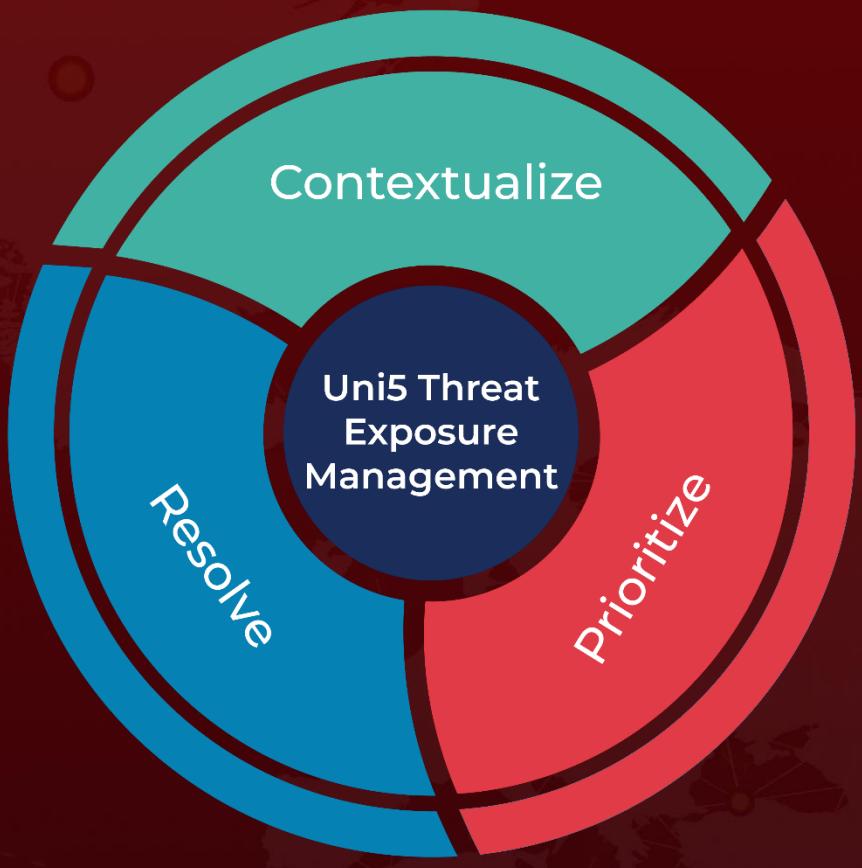
References

https://www.silentpush.com/blog/the-1877-team-a-kurdish-hacker-group-on-the-rise

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

May 4, 2023 • 7:15 AM

More at www.hivepro.com