Hive Pro

Threat Level

Amber

THREAT ADVISORY

ATTACK REPORT

Dangerous Savanna campaign attacked African financial institutions

Date of Publication	Admiralty Code	TA Number
September 9, 2022	A1	TA2022198

Summary

For the past two years, a malicious campaign known as DangerousSavanna has been targeting various financial service firms in Africa. The attackers use spear-phishing to infiltrate financial institution employees in at least five different French-speaking countries, including Ivory Coast, Morocco, Cameroon, Senegal, and Togo.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0005** Defense Evasion	**TA0002** Execution	**TA0003** Persistence
TA0009 Collection	**TA0006** Credential Access	**TA0008** Lateral Movement	**TA0011** Command and Control
TA0004 Privilege Escalation	**T1059** Command and Scripting Interpreter	**T1047** Windows Management Instrumentation	**T1547** Boot or Logon Autostart Execution
T1027 Obfuscated Files or Information	**T1055** Process Injection	**T1204** User Execution	**T1056** Input Capture
T1036 Masquerading	**T1187** Forced Authentication	**T1021** Remote Services	**T1569** System Service
T1053 Scheduled Task/Job	**T1127** Trusted Developer Utilities Proxy Execution	**T1530** Data from Cloud Storage Object	**T1102** Web Service
T1566 Phishing			

Technical Details

#1

DangerousSavanna often deploys relatively simple software tools in compromised systems. These tools are self-written as well asbased on open-source projects like Metasploit, PoshC2, DWservice, and AsyncRAT. The infection begins with the distribution of spear-phishing emails written in French..

#2

The phishing emails contain Word or PDF attachments that entice the user to download and then manually execute the next stage. The basic flow employs Word documents with macros that put an LNK file in the Startup folder. When the LNK file is executed, it downloads from the server and runs PowerShell operations to bypass AMSI and eventually install the PoshC2 implant to control the infected machines.

#3

PowerShell is launched after the initial infection to download code from a Pastebin-like service called "paste[.]c-net.org" or a dedicated C&C server. The third block of the PowerShell PoshC2 implant has a backdoor that communicates with the C&C server. Next, the actors create persistence and perform reconnaissance, as well as run some AMSI bypass commands to try to circumvent detection.

Indicator of Compromise (IOC)

TYPE	VALUE
MD5	020ea21556b56229bb9714e721d893df 0789e52f16f5fc4ac2dbebadf53d44ec 0b1d7c043be8c696d53d63fc0c834195 16157cdfd7b0ea98c44df15fb2fcb417 1818f84f7f51be74a408f5e193ba5908 18889d70d5546b861c6fa4ec11126942 192b70891de0d54af6fa46bd35a5fd87 1ccd2ce1e827b598207cc65e16686b7b 1eb29f64f19e07d42d9ad8f6597424b8 1eed3153b1afae1676ebd0db99ac5802 1f4f537e550e4299a945a97c1f8a0441 28165bb98959e7e7d9be67f0d248b31d 2c95e83759487d78070b56e40843c543 2e7c90c45b3cd8db15cd22e0caacfd40 31515f871cb12d538d53e730e5ddd406 3227c8a45ce4ccf8c475a51b331720c1 3c70bc09d1f8033e57323879d50ca3ce 40ec0d84272f1f2394b4a3b74dafbf70

TYPE	VALUE
IPV4	15.236.51[.]204 3.8.126[.]182 35.181.50[.]113 13.37.250[.]144 13.38.90[.]3 137.116.142[.]70 170.130.172[.]46 192.18.141[.]199 20.70.163[.]11 192.9.244[.]42 20.194.195[.]96
URLs	iplogger[.]org/2zaEa6 bit[.]ly/PDF_MicrosoftOnline cdn.filesend[.]jp/private/hTsvHkbWaUSEZ7ilocBGMTgumxqFmSrVgF-9Ht5LL6YCf4A7Eu28rIxdbo-ND_F9/Chimers.gif 4sync[.]com/web/directDownload/QHZsERS6/rHb0lMWD.f2e6a9154ab6cd29b337d6b555367580 4sync[.]com/web/directDownload/rE33SDmE/iNXXJkWJ.4bf28df12d9e7d99bc902edb6d23c6e2 raw.githubusercontent[.]com/R3mEm/vox/main/vox.ps1 paste.c-net[.]org/CookiesEstrogen paste.c-net[.]org/ExportDeposit paste.c-net[.]org/OrientalAntonio paste.c-net[.]org/ShaveDavie paste.c-net[.]org/SidingFatigue paste.c-net[.]org/HearingsGuided paste.c-net[.]org/SelvesGangster paste.c-net[.]org/StaceConcerns paste.c-net[.]org/BogeyUglier paste.c-net[.]org/MuggingFunny paste.c-net[.]org/NelsonTasteful paste.c-net[.]org/ShaveDie paste.c-net[.]org/GiovanniKismet

References

https://research.checkpoint.com/2022/dangeroussavanna-two-year-long-campaign-targets-financial-institutions-in-french-speaking-africa/

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Continuous Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.

At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

September 9, 2022 • 5:45 AM

© 2022 All Rights are Reserved by HivePro

More at www.hivepro.com