CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

July 16, 2024

TAG-100 Uses Open-Source Tools in Suspected Global Espionage Campaign, Compromising Two Asia-Pacific Intergovernmental Bodies

TAG-100 has targeted high-profile government and private sector organizations globally in a suspected cyber-espionage campaign.

The group employs open-source remote access capabilities and exploits a wide range of internet-facing appliances for initial access, including enterprise VPN, firewall, and email appliances.

TAG-100 compromised two major Asia-Pacific intergovernmental organizations, as well as diplomatic, government, semiconductor supply-chain, non-profit, and religious organizations in over ten countries.

Note: The analysis cut-off date for this report was May 11, 2024

Executive Summary

Recorded Future's Insikt Group identified new suspected cyber-espionage activity targeting high-profile government, intergovernmental, and private sector organizations globally. This activity, which we are tracking under the temporary group designator TAG-100, has employed open-source remote access capabilities and exploited a wide range of internet-facing appliances for initial access. Using Recorded Future® Network Intelligence data, Insikt Group identified the likely compromise of the secretariats of two major Asia-Pacific intergovernmental organizations by TAG-100 using the open-source, multi-platform Go backdoor Pantegana. Other targeted organizations include multiple diplomatic entities and ministries of foreign affairs, as well as industry trade associations and semiconductor supply-chain, non-profit, and religious organizations globally. At this time, Insikt Group is continuing to explore potential attribution for this activity; however, the specific targeting and victimology identified align with a suspected espionage motive.

This activity highlights the ability to combine weaponized proof-of-concept (PoC) exploits with open-source post-exploitation frameworks such as Pantegana, lowering the entry barrier for less capable threat actors. It also allows higher-tier groups to refrain from using customized tools during operations in which they are less concerned with being detected or in which heightened attribution obfuscation is desirable. More widely, threat actors' exploitation of vulnerable internet-facing devices has been the focus of international cybersecurity efforts, including emergency patch requests within the United States (US), the introduction of secure-by-design legislation by the United Kingdom (UK) government, and attributing the use of this technique to multiple state-sponsored threat actors (1, 2, 3). Despite this attention, this form of initial access continues to be widely used, as these devices typically have limited visibility, logging capabilities, and support for traditional security solutions. As a result, it exposes many organizations to the financial downsides of successful attacks, such as operational downtime, reputational damage, and regulatory fines.

Organizations should employ intelligence-led patching prioritization of perimeter appliances that consider the public availability of exploit code, as this availability can substantially increase the likelihood of mass exploitation (1, 2, 3). Organizations should focus on regularly auditing internet-facing and perimeter appliances, reducing their attack surfaces by disabling interfaces or portals where not required, and improving defense-in-depth measures focusing on detecting post-exploitation persistence, discovery, and lateral movement. Unless the security of internet-facing devices is improved or organizations take steps to move away from vulnerable edges, these devices will almost certainly continue to be widely exploited by a range of threat actors.

State-sponsored threat actors will likely continue using open-source capabilities to conduct higher-tempo, deniable cyber operations with a lower risk of direct attribution or retaliation. The widespread availability of open-source capabilities also allows state-sponsored threat actors to outsource select cyber operations to a broader range of less capable proxy groups or private

contractors who may not possess or require in-house development skills due to the widespread availability of open-source tools. This outsourcing will likely act as a force multiplier to further increase the intensity and tempo of overall activity targeting enterprise networks, a trend already apparent within some state-sponsored cyber-espionage programs.

Key Findings

- TAG-100 has likely compromised organizations in at least ten countries in Africa, Asia, North America, South America, and Oceania and, following initial access, employed the open-source Go backdoors Pantegana and SparkRAT.
- TAG-100 has also conducted probable reconnaissance and exploitation activity targeting the internet-facing appliances of additional organizations in at least fifteen countries in North America, Europe, and Asia.
- Based on the identified TAG-100 targeted and victim hosts, it is likely that the group has exploited a range of internet-facing products, including Citrix NetScaler ADC and Gateway appliances, F5 BIG-IP, Zimbra Collaboration Suite, Microsoft Exchange, SonicWall, Cisco Adaptive Security Appliances (ASA), Palo Alto Networks GlobalProtect, and Fortinet FortiGate.
- In the immediate aftermath of releasing a PoC exploit for Palo Alto Networks GlobalProtect firewall vulnerability CVE-2024-3400, TAG-100 conducted probable reconnaissance and attempted exploitation against dozens of US-based organizations running these devices.
- The widespread targeting of internet-facing appliances is particularly attractive because it offers a foothold within the targeted network via products that often have limited visibility, logging capabilities, and support for traditional security solutions, reducing the risk of detection post-exploitation.

Threat Analysis

Wide Range of Strategic Global Targets Compromised

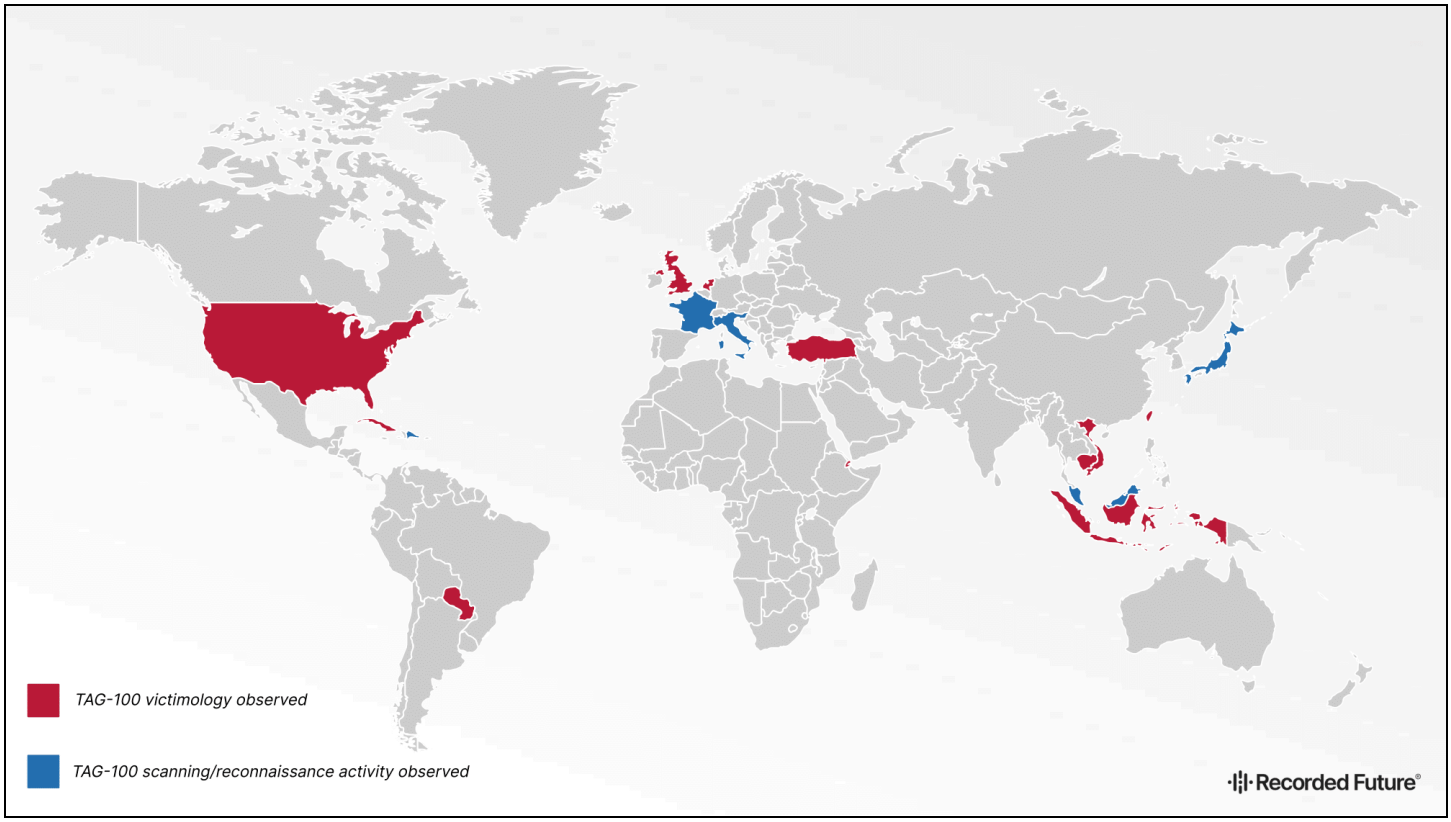

Figure 1: *Geographical breakdown of TAG-100 targeting and victimology (Source: Recorded Future)*

Since at least February 2024, Insikt Group has identified likely victim organizations in Cambodia, Djibouti, the Dominican Republic, Fiji, Indonesia, Netherlands, Taiwan, the United Kingdom, the United States, and Vietnam communicating with TAG-100 command-and-control (C2) infrastructure. Victims included industry trade associations as well as government, intergovernmental, diplomatic, political, semiconductor supply-chain, non-profit, and religious organizations across these countries, including the following notable organizations:

- Intergovernmental organizations headquartered in Southeast Asia and Oceania
- Ministries of Foreign Affairs of countries in Southeast Asia, South America, and the Caribbean
- The Embassy of a Southwest Asian country in the United States
- Multiple religious organizations in the US and Taiwan
- A US-based financial industry trade association
- A Taiwanese semiconductor testing and assembly company

Most victim IP addresses host internet-facing appliances, including Citrix NetScaler ADC and Gateway, Zimbra Collaboration Suite, Microsoft Exchange, SonicWall, Cisco ASA, and Fortinet FortiGate products.

TAG-100 Exploitation of Internet-Facing Appliances

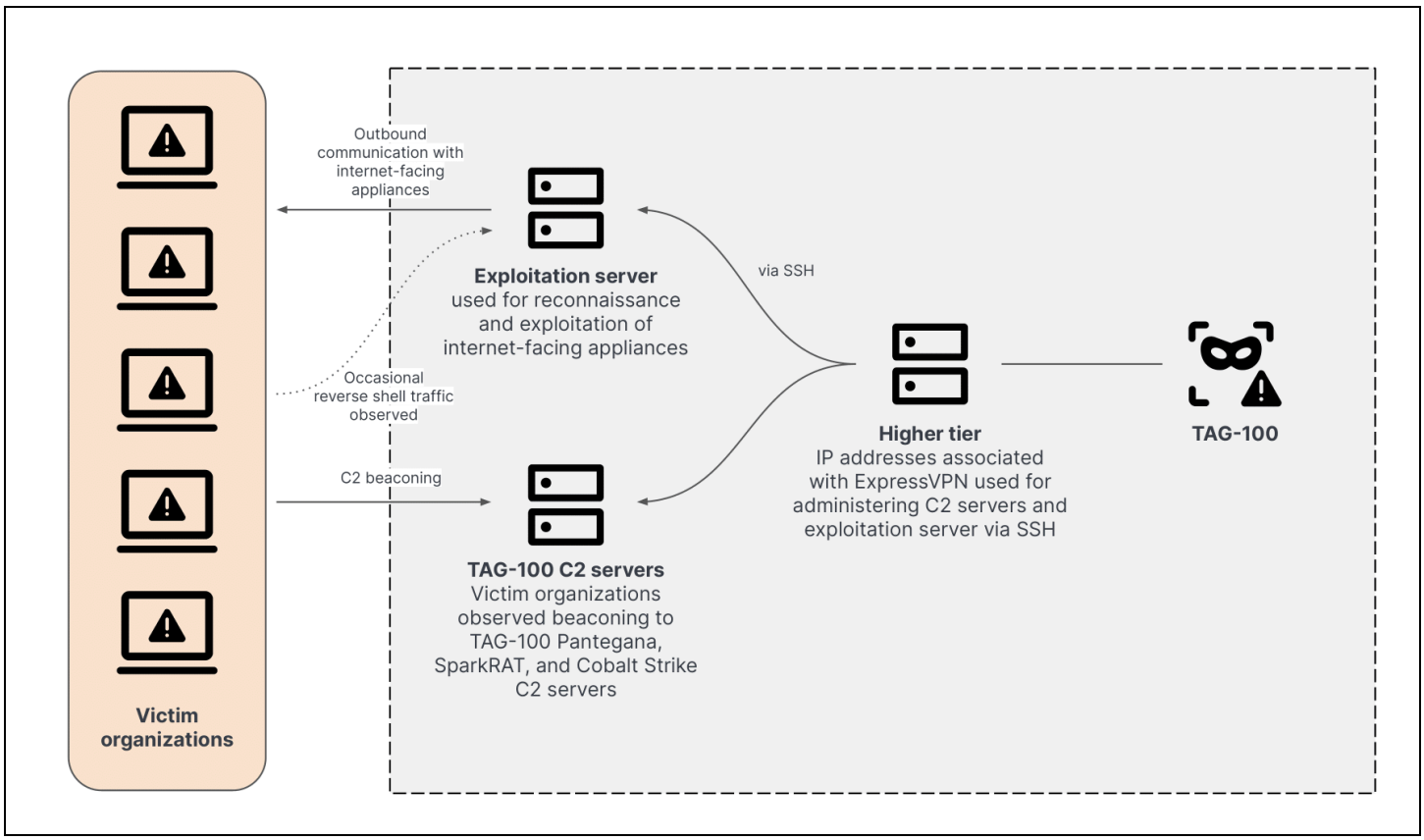

Figure 2: *Overview of TAG-100 operations (Source: Recorded Future)*

TAG-100 has conducted reconnaissance and exploitation activity targeting a wide range of internet-facing appliances belonging to organizations in at least fifteen countries, including Cuba, France, Italy, Japan, and Malaysia. Notably, this included the targeting of multiple Cuban embassies, including in Bolivia, France, and the United States.

In March 2024, TAG-100 was identified targeting internet-facing Citrix NetScaler and F5 BIG-IP appliances and Outlook Web App login portals globally. In multiple instances, these targeted organizations directly overlapped with subsequent victims communicating with TAG-100 Pantegana C2 servers.

Beginning on April 16, 2024, TAG-100 conducted probable reconnaissance and exploitation activity targeting Palo Alto Networks GlobalProtect appliances of organizations, mostly based in the US, within the education, finance, legal, local government, and utilities sectors. The timing of this activity aligned

with the release of a PoC exploit for the Palo Alto Networks GlobalProtect firewall remote code execution vulnerability CVE-2024-3400.

In one instance, an open directory present on the staging server attributed to TAG-100, *209.141.57[.]75*, contained a publicly available exploit for the Zimbra Collaboration Suite vulnerability CVE-2019-9621.

Employing Multiple Open-Source and Offensive Security Capabilities

In addition to employing publicly available exploits, TAG-100 has also used multiple open-source or offensive security post-exploitation frameworks targeting multiple operating systems, including Pantegana, SparkRAT, LESLIELOADER, Cobalt Strike, and CrossC2.

Pantegana

Pantegana is an open-source malware family written in Go that features a cross-platform payload client (Windows, Linux, OSX) and uses HTTPS for C2 communications. It supports file upload and download, system fingerprinting, and direct command-line interaction with infected hosts. Pantegana also supports obfuscation using the open-source obfuscator Garble. Publicly reported use of Pantegana in the wild to date is minimal, other than a campaign exploiting a zero-day vulnerability in the Sophos Firewall appliance attributed by Volexity to the suspected Chinese state-sponsored threat activity group DriftingCloud.

In March 2024, Insikt Group identified a cluster of TAG-100 C2 servers, all exhibiting the same self-signed transport layer security (TLS) certificate (see **Appendix C**), which aligns with the default issuer and distinguished names seen in the Pantegana source code. On some TAG-100 Pantegana servers, the group also employed a customized TLS certificate, which used the organization name `Google, Inc.` rather than the default `Pantegana` value.

All identified TAG-100 servers were running identical services and were administered via the same nodes associated with the commercial VPN service ExpressVPN. Several victim organizations have been observed communicating with multiple TAG-100 Pantegana C2 servers over time, likely because the threat actor transitioned between an older C2 server and a newer one.

SparkRAT and LESLIELOADER

Multiple TAG-100 servers were concurrently linked to malware samples of another open-source Go backdoor, SparkRAT. TAG-100 also used a variant of the publicly available Go loader LESLIELOADER to load SparkRAT in several instances, including a chain previously documented in March 2024 Kroll research. On one occasion, we also observed a SparkRAT memory dump uploaded to a public malware repository that almost certainly originated from a Djibouti government network compromised by TAG-100.

In addition to communicating with a C2 IP address serving a specific Pantegana TLS certificate linked to TAG-100, the Linux SparkRAT sample `Sync` shown in **Table 1** was also identified being staged on a

previously referenced TAG-100 open directory on the IP address *209.141.57[.]75* between November 2023 and April 2024.

SHA256 Hash	Filename	C2 IP Address
23efecc03506a9428175546a4b7d40c8a943c252110e83dec132c6a5db8c4dd6	Sync	216.238.68[.]36
ec45da0ca70a9b71652cc95d51665f7ad568294bd5652c395a119bccd613e9b4	Ntmssvc.dll	209.141.50[.]215
b8cab11421eb4731c16cf3c34ca2b3f2a758d5e112f877b90a18b3e146c8add0	RemovableStorage.dll	209.141.50[.]215

Table 1: *TAG-100 SparkRAT samples (Source: Recorded Future)*

Cobalt Strike

TAG-100 has used both traditional Windows Cobalt Strike Beacon payloads using the Jquery malleable C2 profile as well as the open-source, cross-platform CrossC2 to generate Cobalt Strike Beacon payloads for Linux systems. The C2 domain used in highlighted TAG-100 Cobalt Strike samples shown in **Table 2**, *www.megtech[.]xyz*, was proxied via CloudFlare content distribution network (CDN) to a backend, threat actor-controlled server administered via ExpressVPN, similar to wider TAG-100 activity. Both samples shown in **Table 2** were also staged on the previously referenced TAG-100-controlled server *209.141.57[.]75*.

SHA256 Hash	Filename	C2 Domain
e3aab908800cb4601bc4a87ac9ac48d816ced57cdb409b6e2468956cc50bdf04	test	www.megtech[.]xyz
8eb3617768ce4693b726bb8187e5cccea3359de0196d6f2bbe555c31f12d1234	svhost.exe	www.megtech[.]xyz

Table 2: *TAG-100 Cobalt Strike samples (Source: Recorded Future)*

Considering TAG-100 Attribution

While Insikt Group cannot attribute TAG-100 activity based on current evidence, the group's consistent targeting of intergovernmental, diplomatic, and religious organizations aligns with a suspected espionage motive. Additionally, several targets of this activity align with historical targeting from Chinese state-sponsored groups, including Asia-Pacific intergovernmental and diplomatic entities, religious organizations in the United States and Taiwan, and a political party that has supported an investigation into the treatment of the Uyghur people by the Chinese government. Despite this, TAG-100's use of open-source tooling coupled with the group's pattern of life, targeting, and broader

tactics, techniques, and procedures (TTPs) provide some conflicting evidence, leading us to continue investigating potential attribution for this activity.

Mitigations

- Configure your intrusion detection systems (IDS), intrusion prevention systems (IPS), or any network defense mechanisms in place to alert on — and upon review, consider blocking connection attempts to and from — the external IP addresses and domains linked in **Appendix A**.
- Ensure security monitoring and detection capabilities are in place for all external-facing services and devices. Monitor for follow-on activity likely to occur following exploitation of these external-facing services, such as the deployment of web shells, backdoors, or reverse shells, as well as subsequent lateral movement to internal networks.
- Ensure a risk-based approach for patching vulnerabilities, prioritizing high-risk vulnerabilities and those exploited in the wild as determined through the Recorded Future® Vulnerability Intelligence module. Regarding Chinese state-sponsored groups, pay particular attention to remote code execution (RCE) vulnerabilities in external-facing appliances within your environment.
- Practice network segmentation and ensure special protections exist for sensitive information; consider implementing multi-factor authentication and extremely restricted access and storage on systems only accessible via an internal network.
- Detect and block malicious infrastructure such as Pantegana, SparkRAT, and Cobalt Strike C2 servers in real-time via the Recorded Future® Threat Intelligence module.
- Recorded Future® Third-Party Intelligence module users can monitor real-time output to identify suspected targeted intrusion activity involving key vendors and partners within physical, network, and software supply chains.
- By monitoring Malicious Traffic Analysis (MTA), Recorded Future clients can alert on and proactively monitor infrastructure involved in notable communication to known TAG-100 C2 IP addresses.

Outlook

The identified TAG-100 activity focused on targeting a variety of internet-facing appliances for initial access and, subsequently, used open-source capabilities post-exploitation. The group has been particularly interested in targeting government and intergovernmental organizations in Southeast Asia, Europe, and North America. This activity further highlights an established trend of threat actors persistently targeting internet-facing appliances for initial access. These appliances are particularly attractive because they offer a foothold within the targeted network via products that often have limited visibility, logging capabilities, and support for traditional security solutions, reducing the risk of detection during post-exploitation activity. The prevalence of this activity has motivated both the US and UK governments to issue parallel efforts to improve security in enterprise software and devices. However, it will likely take time before the effects of this top-down approach are fully realized. In the meantime, vulnerable network edges will almost certainly continue to be heavily exploited by financially motivated and state-sponsored threat actors as long as organizations deploy them.

Appendix A — Indicators of Compromise

TAG-100 C2 Infrastructure

IP Address	First Seen	Last Seen
209.141.46[.]83	2024-03-04	2024-05-11
209.141.57[.]75	2023-01-30	2024-04-24
205.185.126[.]208	2024-03-10	2024-04-07
38.54.115[.]34	2024-02-18	2024-03-07
209.141.42[.]131	2024-02-20	2024-03-03
104.244.79[.]119	2023-11-01	2024-01-27
207.246.108[.]119	2024-01-08	2024-01-21
38.54.15[.]164	2023-09-06	2024-01-20
198.98.49[.]41	2023-12-03	2024-01-08
209.141.50[.]215	2023-11-09	2023-12-04
205.185.127[.]12	2023-02-06	2023-11-21
209.141.50[.]215	2023-11-09	2023-11-21
45.32.107[.[53	2023-09-04	2023-09-18
205.185.117[.]73	2023-01-10	2023-07-12
216.238.68[.]36	2023-05-04	2023-06-12
209.141.37[.]217	2023-04-14	2023-05-25
205.185.121[.]169	2023-04-14	2023-05-01
144.202.125[.]201	2023-04-12	2023-04-18
173.254.229[.]93	2023-01-09	2023-01-09

TAG-100 Exploitation Servers

IP Address	First Seen	Last Seen
205.185.122[.]35	2024-04-21	2024-05-11
209.141.47[.]6	2024-02-03	2024-05-11

TAG-100 Cobalt Strike C2 Domain

www.megtech[.]xyz

Pantegana Self-signed TLS Certificate Fingerprint

9b6bc9e7ed924900e5dfb8df2ac0916fbe6913a7717c341152f5c17ae017278c

Cobalt Strike Samples (SHA256)

e3aab908800cb4601bc4a87ac9ac48d816ced57cdb409b6e2468956cc50bdf04
8eb3617768ce4693b726bb8187e5cccea3359de0196d6f2bbe555c31f12d1234

SparkRAT/LESLIELOADER Samples (SHA256)

23efecc03506a9428175546a4b7d40c8a943c252110e83dec132c6a5db8c4dd6
ec45da0ca70a9b71652cc95d51665f7ad568294bd5652c395a119bccd613e9b4
b8cab11421eb4731c16cf3c34ca2b3f2a758d5e112f877b90a18b3e146c8add0

Appendix B — MITRE ATT&CK Techniques

Tactic: Technique	ATT&CK Code
Resource Development: Acquire Infrastructure: Virtual Private Server	T1583.003
Reconnaissance: Active Scanning: Vulnerability Scanning	T1595.002
Initial Access: Exploit Public-Facing Application	T1190
Defense Evasion: Process Injection	T1055
Defense Evasion: Obfuscated Files or Information: Embedded Payloads	T1027.009
Defense Evasion: Obfuscated Files or Information: Encrypted/Encoded File	T1027.013
Command and Control: Application Layer Protocol: Web Protocols	T1071
Command and Control: Web Service: Bidirectional Communication	T1102.002

Appendix C — Self-Signed Pantegana TLS Certificate Observed on TAG-100 Infrastructure

```
Version:          3 (0x02)
Serial number:    706010028792834994577798306374710690671657412 29
Algorithm ID:     SHA256withRSA
Validity
  Not Before:     24/10/2022 06:08:04
  Not After:      21/10/2032 06:08:04
Issuer
  C  = US
  ST = Hawaii
  L  = The Sewers
  O  = Pantegana, Inc.
  CN = Pantegana Root CA
Subject
  C  = US
  ST = Hawaii
  L  = The Sewers
  O  = Pantegana, Inc.
  CN = localhost
Public Key
  Algorithm:      RSA
  Length:         2048 bits
  Modulus:        bf:66:12:ec:36:4d:54:62:f0:4b:c7:44:f2:8a:39:ca:
                  06:9a:7f:e0:dc:9a:c3:55:77:b4:4f:41:a2:ed:db:57:
                  a2:03:99:b4:8e:70:9c:07:88:d7:b2:cd:42:b6:88:15:
                  cb:0b:70:26:90:5b:18:17:a8:4d:a7:7a:a0:0f:f9:71:
                  bb:4f:1f:21:ac:41:a4:2b:b5:1d:12:f8:32:46:56:2c:
                  d9:11:09:f3:ac:39:75:aa:39:1d:37:b3:88:72:c6:c1:
                  e9:06:3d:ae:d4:c5:9d:30:54:cb:4d:2d:86:b6:7a:9f:
                  9c:03:90:5d:24:d9:36:e2:40:b9:f0:7e:08:8b:c6:81:
                  e8:6c:76:cd:f4:2e:95:10:11:ad:3b:7d:72:7c:01:a7:
                  cb:85:39:40:25:cb:0a:c8:b4:5a:46:e6:23:99:9c:64:
                  ee:1d:2c:0b:64:a7:ef:75:dd:37:96:e0:34:9f:54:28:
                  9f:6e:cc:6c:48:0f:74:6f:c8:11:26:3b:95:23:bb:e4:
                  6f:df:8b:86:38:c9:7e:79:e5:fc:f2:4a:01:30:68:e0:
                  12:de:af:3b:3d:19:bc:b4:e0:88:52:97:4a:70:62:4c:
                  93:31:fa:5b:5f:a2:46:b4:2b:ec:a0:c2:19:d4:29:70:
                  0d:d6:1f:31:28:79:6f:24:26:83:66:dd:d7:51:a0:2d
  Exponent:       65537 (0x10001)
Certificate Signature
  Algorithm:      SHA256withRSA
  Signature:      ad:8f:be:9c:32:9f:da:6c:ab:8f:48:93:50:c6:47:84:
                  33:c1:ec:63:97:28:1a:f4:b6:ad:02:a1:8e:94:bd:82:
                  66:0b:45:b1:19:f1:2a:36:35:96:44:2a:ec:e9:29:76:
                  f4:b1:2d:e8:cd:e6:fd:32:40:6a:ab:6a:ee:07:84:a6:
                  5f:4a:20:66:8c:8b:df:f1:b5:a0:ae:d9:86:e1:ea:01:
                  58:e0:91:63:77:4d:d9:b1:3c:e2:3d:5a:2d:25:2c:80:
                  c6:db:1b:42:f7:3a:d3:2e:56:fc:13:fe:33:cc:2e:57:
```

```
                  5d:fd:01:1b:d5:23:9b:3a:c0:1a:e0:68:10:37:63:56:
                  d5:c2:57:c9:f8:38:ef:42:61:0a:cb:62:70:a2:3c:17:
                  df:67:0c:eb:d5:5d:b1:d7:5b:f8:e4:17:c5:62:1e:68:
                  8b:0b:0e:2d:ad:82:c3:00:af:0a:f5:a3:de:5d:22:34:
                  ed:e9:52:4c:75:7f:16:26:48:af:bb:51:a6:ea:f3:ff:
                  d9:f4:b6:e7:2b:60:fc:01:cd:8a:08:e1:da:2d:19:b9:
                  3c:b9:8b:90:25:07:23:5f:16:1e:60:cc:10:75:6b:65:
                  33:e0:99:51:21:9d:c4:fa:5a:f2:30:0f:72:81:72:45:
                  f3:b9:b8:37:40:ee:c9:3e:5a:94:bb:20:56:c0:58:92

Extensions
  subjectAltName :
    dns: localhost
    ip: 127.0.0.1
```

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,800 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com