Mar 05 2024

NETMANAGEIT

Intelligence Report

A comprehensive analysis of I-Soon's commercial offering

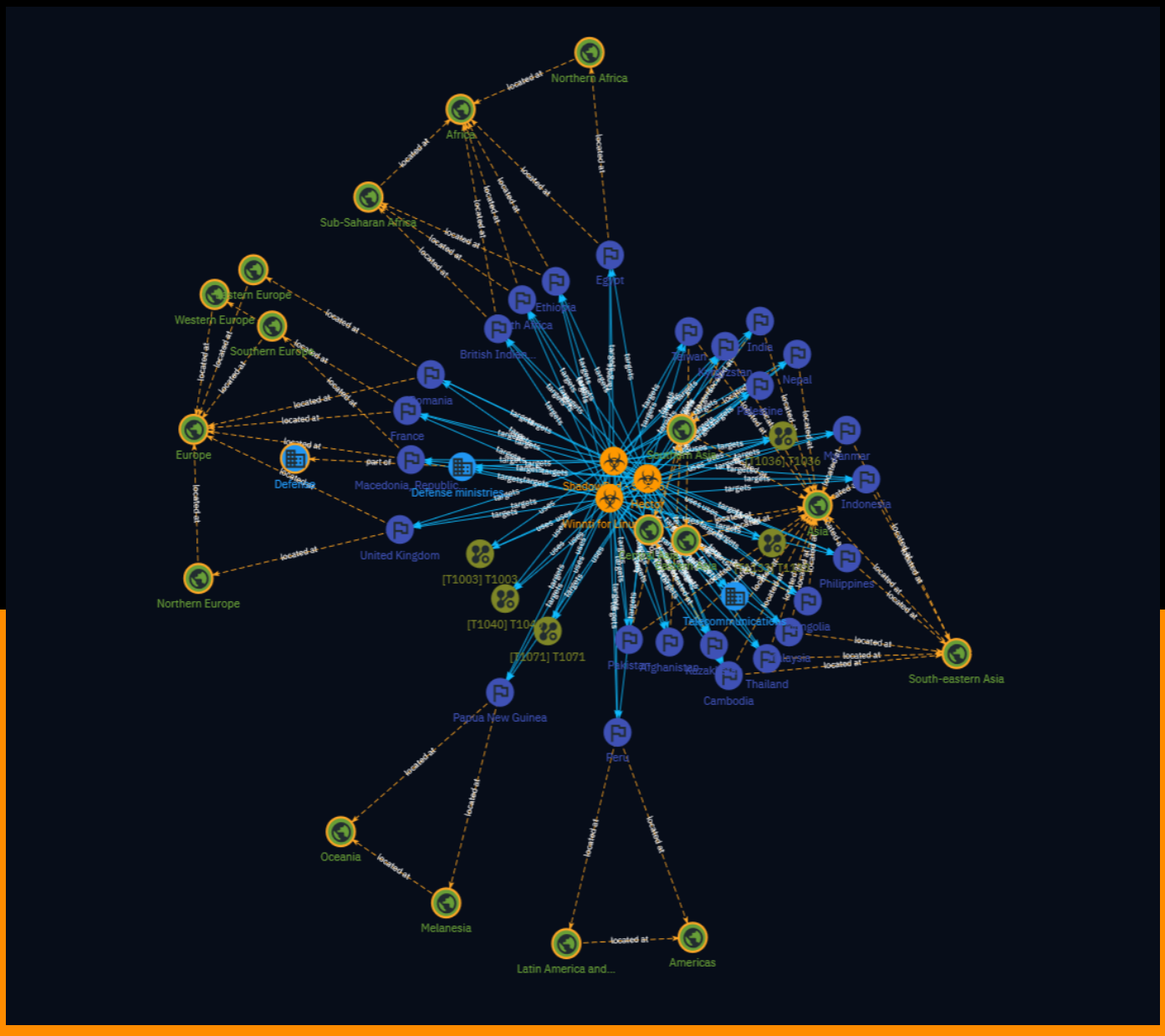

Table of contents

Overview

Entities

External References

Overview

Description

This report provides an in-depth analysis of leaked documents pertaining to I-Soon, a Chinese cybersecurity company linked to state-sponsored hacking operations. The leaks offer unprecedented insight into I-Soon's capabilities, victim targeting, and links to known APT campaigns. Key findings include I-Soon's focus on data exploitation platforms, lack of sophistication in intrusion methods despite success breaching strategic targets worldwide, and autonomy in conducting speculative compromises. The report assesses damage from the leaks and provides historical context around I-Soon's role in China's public-private cybersecurity apparatus.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

100 / 100

Content

N/A

Malware

Name
Hector
Name
Winnti for Linux - S0430
Name
ShadowPad - S0596

Country

Name
Palestine
Name
Papua New Guinea
Name
France
Name
Macedonia, Republic of
Name
United Kingdom
Name
Romania
Name
Nepal

Name
Pakistan
Name
India
Name
Afghanistan
Name
Philippines
Name
Thailand
Name
Myanmar
Name
Malaysia
Name
Cambodia
Name
Indonesia

Name
Taiwan
Name
Mongolia
Name
Kyrgyzstan
Name
Kazakhstan
Name
Peru
Name
South Africa
Name
Ethiopia
Name
British Indian Ocean Territory
Name
Egypt

Attack-Pattern

Name
T1036
ID
T1036
Description
Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names. Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site) Masquerading may also include the use of [Proxy](https://attack.mitre.org/techniques/T1090) or VPNs to disguise IP addresses, which can allow adversaries to blend in with normal network traffic and bypass conditional access policies or anti-abuse protections.
Name
T1071
ID
T1071

Description

Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.

Name

T1040

ID

T1040

Description

Adversaries may sniff network traffic to capture information about an environment, including authentication material passed over the network. Network sniffing refers to using the network interface on a system to monitor or capture information sent over a wired or wireless connection. An adversary may place a network interface into promiscuous mode to passively access data in transit over the network, or use span ports to capture a larger amount of data. Data captured via this technique may include user credentials, especially those sent over an insecure, unencrypted protocol. Techniques for name service resolution poisoning, such as [LLMNR/NBT-NS Poisoning and SMB Relay](https://attack.mitre.org/techniques/T1557/001), can also be used to capture credentials to websites, proxies, and internal systems by redirecting traffic to an adversary. Network sniffing may also reveal configuration details, such as running services, version numbers, and other network characteristics (e.g. IP addresses, hostnames, VLAN IDs) necessary for subsequent Lateral Movement and/or Defense Evasion activities. In cloud-based environments, adversaries may still be able to use traffic mirroring services to sniff network traffic from virtual machines. For example, AWS Traffic Mirroring, GCP Packet Mirroring, and Azure vTap allow users to define specified instances to collect traffic from and specified targets to send collected traffic to.(Citation: AWS Traffic Mirroring)(Citation: GCP Packet Mirroring)(Citation: Azure Virtual Network TAP) Often, much of this traffic will be in cleartext due to the use of TLS termination at the load balancer level to reduce the strain of encrypting and decrypting traffic.(Citation: Rhino Security Labs AWS VPC Traffic

Mirroring)(Citation: SpecterOps AWS Traffic Mirroring) The adversary can then use exfiltration techniques such as Transfer Data to Cloud Account in order to access the sniffed traffic.(Citation: Rhino Security Labs AWS VPC Traffic Mirroring) On network devices, adversaries may perform network captures using [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `monitor capture`.(Citation: US-CERT-TA18-106A)(Citation: capture_embedded_packet_on_software)

Name

T1133

ID

T1133

Description

Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as [Windows Remote Management](https://attack.mitre.org/techniques/T1021/006) and [VNC](https://attack.mitre.org/techniques/T1021/005) can also be used externally.(Citation: MacOS VNC software for Remote Desktop) Access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) to use the service is often a requirement, which could be obtained through credential pharming or by obtaining the credentials from users after compromising the enterprise network.(Citation: Volexity Virtual Private Keylogging) Access to remote services may be used as a redundant or persistent access mechanism during an operation. Access may also be gained through an exposed service that doesn't require authentication. In containerized environments, this may include an exposed Docker API, Kubernetes API server, kubelet, or web application such as the Kubernetes dashboard.(Citation: Trend Micro Exposed Docker Server)(Citation: Unit 42 Hildegard Malware)

Name

T1003

ID

T1003

Description

Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform [Lateral Movement](https://attack.mitre.org/tactics/TA0008) and access restricted information. Several of the tools mentioned in associated sub-techniques may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.

Region

Name
Melanesia
Name
Oceania
Name
Western Europe
Name
Southern Europe
Name
Northern Europe
Name
Eastern Europe
Name
Europe

Name
Southern Asia
Name
South-eastern Asia
Name
Eastern Asia
Name
Central Asia
Name
Asia
Name
Latin America and the Caribbean
Name
Americas
Name
Sub-Saharan Africa
Name
Northern Africa

Name
Africa

Sector

Name
Telecommunications
Description
Private and public entities involved in the production, transport and dissemination of information and communication signals.
Name
Defense ministries (including the military)
Description
Includes the military and all defense related-space activities.
Name
Defense
Description
Public and private entities involved in the conception and production of weapons and the planning and conducting of military operations.

External References

- https://harfanglab.io/en/insidethelab/isoon-leak-analysis/
- https://otx.alienvault.com/pulse/65e5fd6e0f9cd14db92db5f8