Mar 08 2024

NETMANAGEIT

Intelligence Report

Lord Nemesis Strikes: Supply Chain Attack on the Israeli Academic Sector

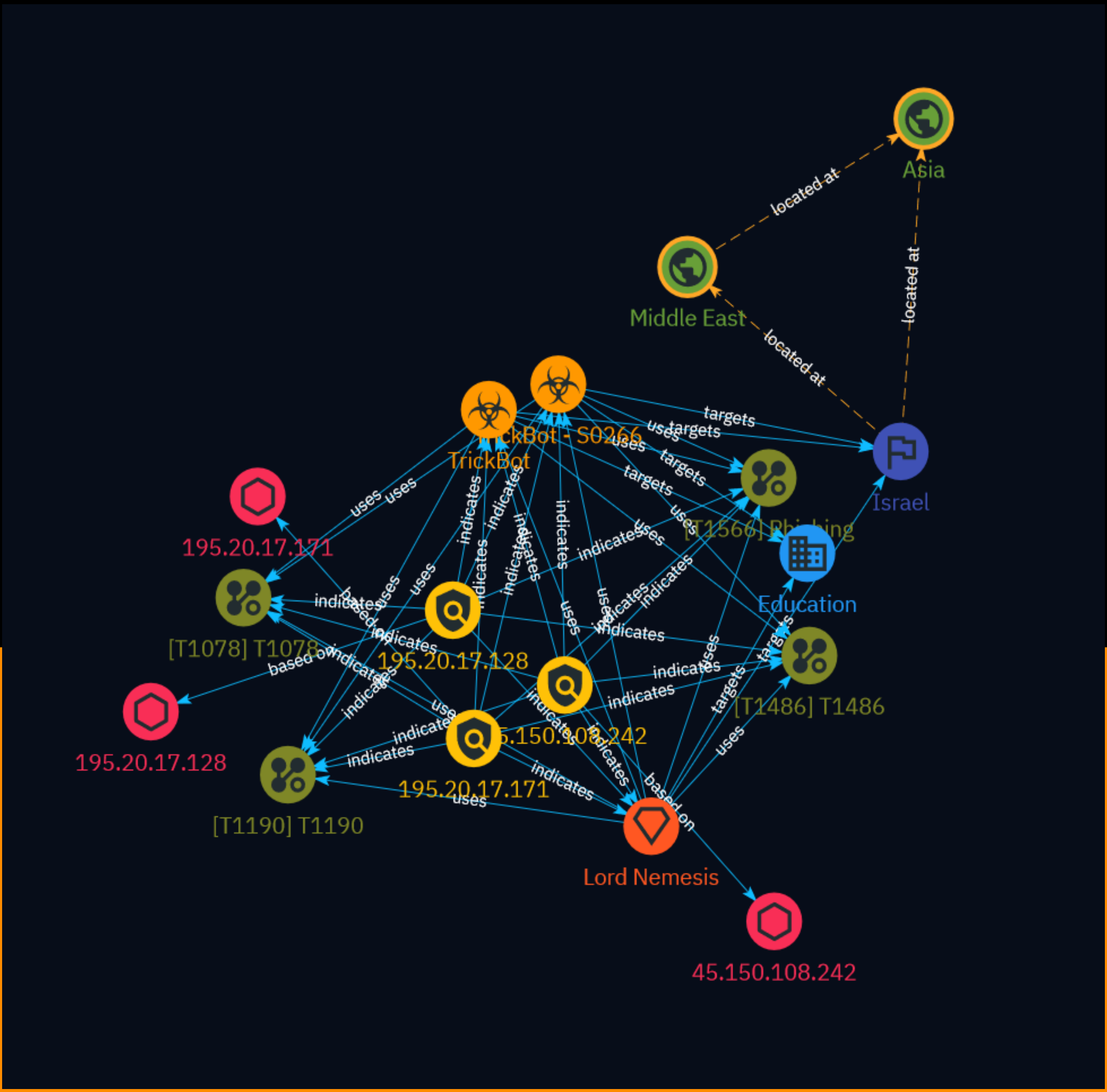

Table of contents

Overview

Entities

Observables

External References

Overview

Description

The Iranian hacktivist group Lord Nemesis recently compromised the systems of Rashim Software, an Israeli provider of academic administration software, and used stolen credentials to breach multiple academic institutions. The group claims to have exfiltrated sensitive data and sent threatening messages to victims. The attack highlights risks from third-party access and the growing threat of nation-state actors targeting smaller organizations for ideological reasons. Expert incident response was required to investigate the breach and provide recommendations to bolster defenses against future hacktivist attacks.

Confidence

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

100 / 100

Content

N/A

Indicator

Name

45.150.108.242

Description

- **Zip Code:** N/A - **ISP:** Interhost Communication Solutions - **ASN:** 61102 - **Organization:** Interhost Communication Solutions - **Is Crawler:** False - **Timezone:** Asia/Jerusalem - **Mobile:** False - **Host:** 45.150.108.242 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** IL - **Region:** Tel Aviv - **City:** Tel Aviv - **Latitude:** 32.08029938 - **Longitude:** 34.7804985

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.150.108.242']

Name

195.20.17.171

Description

- **Zip Code:** N/A - **ISP:** BlueVPS OU - **ASN:** 62005 - **Organization:** BlueVPS OU - **Is Crawler:** False - **Timezone:** Asia/Jerusalem - **Mobile:** False - **Host:** Arshia.cloud - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** IL - **Region:** Central District - **City:** Petah Tikva - **Latitude:** 32.10329819 - **Longitude:** 34.88790131

Pattern Type

stix

Pattern

[ipv4-addr:value = '195.20.17.171']

Name

195.20.17.128

Description

- **Zip Code:** N/A - **ISP:** BlueVPS OU - **ASN:** 62005 - **Organization:** BlueVPS OU - **Is Crawler:** False - **Timezone:** Asia/Jerusalem - **Mobile:** False - **Host:** teddy2012.services-israel.co.il - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** IL - **Region:** Central District - **City:** Petah Tikva - **Latitude:** 32.10329819 - **Longitude:** 34.88790131

Pattern Type

stix

Pattern

[ipv4-addr:value = '195.20.17.128']

Malware

Name

TrickBot - S0266

Name

TrickBot

Description

[TrickBot](https://attack.mitre.org/software/S0266) is a Trojan spyware program written in C++ that first emerged in September 2016 as a possible successor to [Dyre](https://attack.mitre.org/software/S0024). [TrickBot](https://attack.mitre.org/software/S0266) was developed and initially used by [Wizard Spider](https://attack.mitre.org/groups/G0102) for targeting banking sites in North America, Australia, and throughout Europe; it has since been used against all sectors worldwide as part of "big game hunting" ransomware campaigns.(Citation: S2 Grupo TrickBot June 2017)(Citation: Fidelis TrickBot Oct 2016)(Citation: IBM TrickBot Nov 2016)(Citation: CrowdStrike Wizard Spider October 2020)

Intrusion-Set

Name
Lord Nemesis

Attack-Pattern

Name
T1486

ID
T1486

Description
Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.(Citation: US-CERT Ransomware 2016)(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017)(Citation: US-CERT SamSam 2018) In the case of ransomware, it is typical that common user files like Office documents, PDFs, images, videos, audio, text, and source code files will be encrypted (and often renamed and/or tagged with specific file markers). Adversaries may need to first employ other behaviors, such as [File and Directory Permissions Modification](https://attack.mitre.org/techniques/T1222) or [System Shutdown/Reboot](https://attack.mitre.org/techniques/T1529), in order to unlock and/or gain access to manipulate these files.(Citation: CarbonBlack Conti July 2020) In some cases, adversaries may encrypt critical system files, disk partitions, and the MBR.(Citation: US-CERT NotPetya 2017) To maximize impact on the target organization, malware designed for encrypting data may have worm-like features to propagate across a network by leveraging other attack techniques like [Valid Accounts](https://attack.mitre.org/techniques/T1078), [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), and [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002).(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017) Encryption malware may also leverage [Internal

Defacement](https://attack.mitre.org/techniques/T1491/001), such as changing victim wallpapers, or otherwise intimidate victims by sending ransom notes or other messages to connected printers (known as "print bombing").(Citation: NHS Digital Egregor Nov 2020) In cloud environments, storage objects within compromised accounts may also be encrypted.(Citation: Rhino S3 Ransomware Part 1)

Name

T1078

ID

T1078

Description

Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Compromised credentials may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access, network devices, and remote desktop.(Citation: volexity_0day_sophos_FW) Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. Adversaries may choose not to use malware or tools in conjunction with the legitimate access those credentials provide to make it harder to detect their presence. In some cases, adversaries may abuse inactive accounts: for example, those belonging to individuals who are no longer part of an organization. Using these accounts may allow the adversary to evade detection, as the original account user will not be present to identify any anomalous activity taking place on their account.(Citation: CISA MFA PrintNightmare) The overlap of permissions for local, domain, and cloud accounts across a network of systems is of concern because the adversary may be able to pivot across accounts and systems to reach a high level of access (i.e., domain or enterprise administrator) to bypass access controls set within the enterprise.(Citation: TechNet Credential Theft)

Name

Phishing

ID

T1566

Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

T1190

ID

T1190

Description

Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration. Exploited applications are often websites/web servers, but can also include databases (like SQL), standard services (like SMB or SSH), network device administration and management protocols (like SNMP and Smart Install), and any other system with Internet accessible open sockets.(Citation: NVD CVE-2016-6662)(Citation: CIS Multiple SMB Vulnerabilities)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)(Citation: Cisco Blog Legacy Device Attacks)(Citation: NVD CVE-2014-7169) Depending on the flaw being exploited this may also involve [Exploitation for Defense Evasion](https://attack.mitre.org/techniques/T1211). If an application is hosted on cloud-based infrastructure and/or is containerized, then exploiting it may lead to compromise of the underlying instance or container. This can allow an adversary a path to access the cloud or container APIs, exploit container host access via [Escape to Host](https://attack.mitre.org/techniques/T1611), or take advantage of weak identity and access management policies. Adversaries may also exploit edge network infrastructure and related appliances, specifically targeting devices that do not support robust host-based defenses.(Citation: Mandiant Fortinet Zero Day)(Citation: Wired Russia Cyberwar) For websites and databases, the OWASP top 10 and CWE top 25 highlight the most common web-based vulnerabilities.(Citation: OWASP Top 10)(Citation: CWE top 25)

Country

Name
Israel

Region

Name
Middle East

Name
Asia

Sector

Name
Education
Description
Public or private entities operating to facilitate learning and acquiring knowledge and skills, composed of infrastructures and services to host teachers, students, and administrative services related to this activity. This does not include research activities.

IPv4-Addr

Value
195.20.17.171
45.150.108.242
195.20.17.128

External References

- https://op-c.net/blog/lord-nemesis-strikes-supply-chain-attack-on-the-israeli-academic-sector/
- https://otx.alienvault.com/pulse/65eb3f576bf818fdf7d1d2d2