Jul 13 2023

NETMANAGEIT

Intelligence Report

Stories from the SOC: OneNote MalSpam – Detection & Response

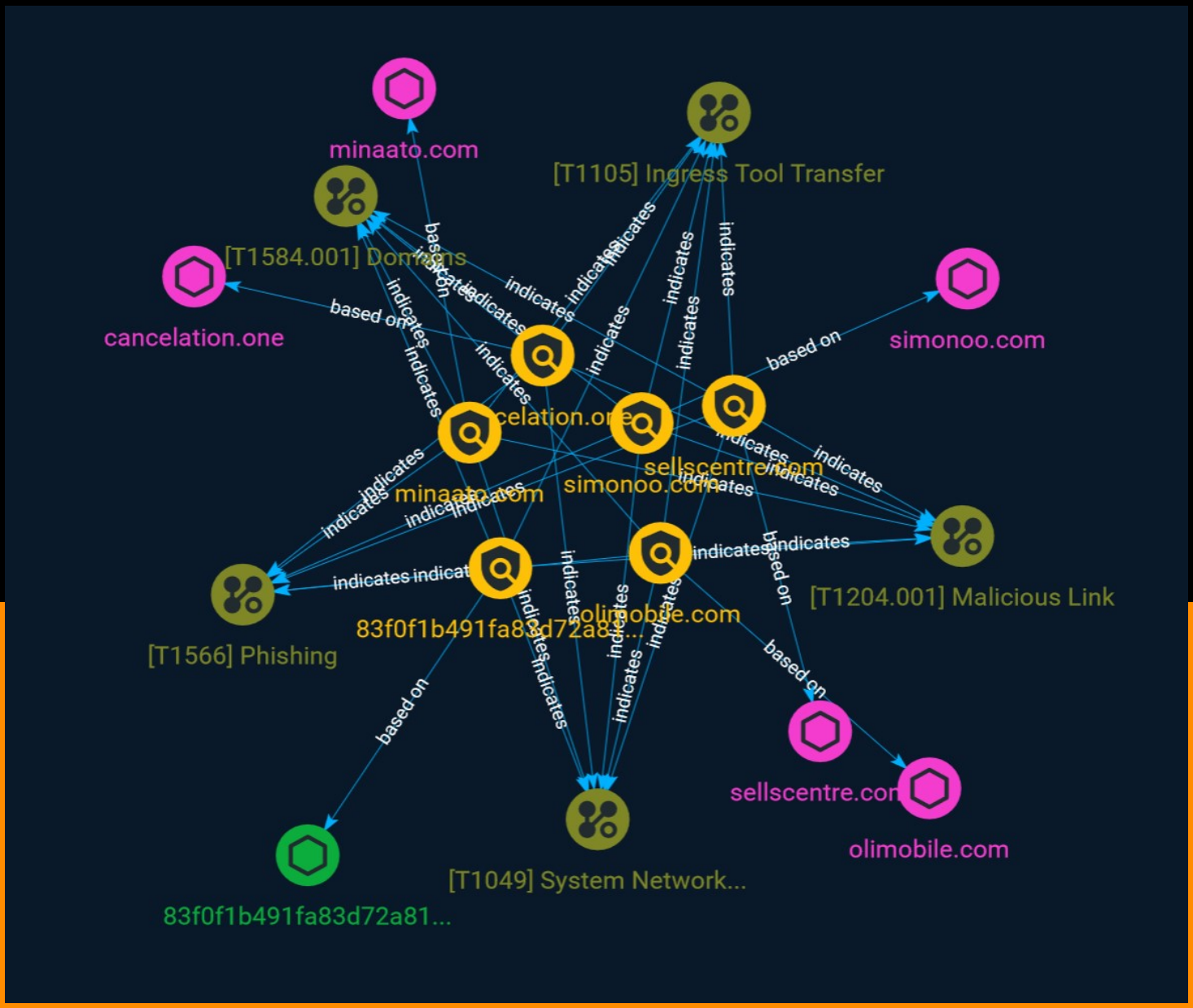

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A look at some of the highlights of AT&T's latest cybersecurity research and development, as well as the findings of a review based on Malspam discovered in a customer's environment.

Confidence

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

15 / 100

Indicator

Name
simonoo.com
Pattern Type
stix
Pattern
[domain-name:value = 'simonoo.com']
Name
83f0f1b491fa83d72a819e3de69455a0b20c6cb48480bcd8cc9c64dbbbc1b581
Description
SHA256 of 8f4fc0dbf3114200e18b7ef23f2ecb0b31a96cd7
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' = '83f0f1b491fa83d72a819e3de69455a0b20c6cb48480bcd8cc9c64dbbbc1b581']

Name

cancelation.one

Pattern Type

stix

Pattern

[domain-name:value = 'cancelation.one']

Name

olimobile.com

Pattern Type

stix

Pattern

[domain-name:value = 'olimobile.com']

Name

minaato.com

Pattern Type

stix

Pattern
[domain-name:value = 'minaato.com']
Name
sellscentre.com
Pattern Type
stix
Pattern
[domain-name:value = 'sellscentre.com']

Attack-Pattern

Name
Domains

ID
T1584.001

Description
Adversaries may hijack domains and/or subdomains that can be used during targeting. Domain registration hijacking is the act of changing the registration of a domain name without the permission of the original registrant.(Citation: ICANNDomainNameHijacking) Adversaries may gain access to an email account for the person listed as the owner of the domain. The adversary can then claim that they forgot their password in order to make changes to the domain registration. Other possibilities include social engineering a domain registration help desk to gain access to an account or taking advantage of renewal process gaps.(Citation: Krebs DNS Hijack 2019) Subdomain hijacking can occur when organizations have DNS entries that point to non-existent or deprovisioned resources. In such cases, an adversary may take control of a subdomain to conduct operations with the benefit of the trust associated with that domain.(Citation: Microsoft Sub Takeover 2020) Adversaries who compromise a domain may also engage in domain shadowing by creating malicious subdomains under their control while keeping any existing DNS records. As service will not be disrupted, the malicious subdomains may go unnoticed for long periods of time.(Citation: Palo Alto Unit 42 Domain Shadowing 2022)

Name
Malicious Link

ID

T1204.001

Description

An adversary may rely upon a user clicking a malicious link in order to gain execution. Users may be subjected to social engineering to get them to click on a link that will lead to code execution. This user action will typically be observed as follow-on behavior from [Spearphishing Link](https://attack.mitre.org/techniques/T1566/002). Clicking on a link may also lead to other execution techniques such as exploitation of a browser or application vulnerability via [Exploitation for Client Execution](https://attack.mitre.org/techniques/T1203). Links may also lead users to download files that require execution via [Malicious File](https://attack.mitre.org/techniques/T1204/002).

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

Ingress Tool Transfer

ID

T1105

Description

Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to the victim network through the command and control channel or through alternate protocols such as [ftp](https://attack.mitre.org/software/S0095). Once present, adversaries may also transfer/spread tools between victim devices within a compromised environment (i.e. [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570)). Files can also be transferred using various [Web Service](https://attack.mitre.org/techniques/T1102)s as well as native or otherwise present tools on the victim system.(Citation: PTSecurity Cobalt Dec 2016) On Windows, adversaries may use various utilities to download tools, such as `copy`, `finger`, [certutil](https://attack.mitre.org/software/S0160), and [PowerShell](https://attack.mitre.org/techniques/T1059/001) commands such as `IEX(New-Object Net.WebClient).downloadString()` and `Invoke-WebRequest`. On Linux and macOS systems, a variety of utilities also exist, such as `curl`, `scp`, `sftp`, `tftp`, `rsync`, `finger`, and `wget`. (Citation: t1105_lolbas)

Name

System Network Connections Discovery

ID

T1049

Description

Adversaries may attempt to get a listing of network connections to or from the compromised system they are currently accessing or from remote systems by querying for information over the network. An adversary who gains access to a system that is part of a cloud-based environment may map out Virtual Private Clouds or Virtual Networks in order to determine what systems and services are connected. The actions performed are likely the same types of discovery techniques depending on the operating system, but the resulting information may include details about the networked cloud environment relevant to the adversary's goals. Cloud providers may have different ways in which their virtual networks operate.(Citation: Amazon AWS VPC Guide)(Citation: Microsoft Azure Virtual Network Overview)(Citation: Google VPC Overview) Similarly, adversaries who gain access to network devices may also perform similar discovery activities to gather information about connected systems and services. Utilities and commands that acquire this information include [netstat](https://attack.mitre.org/software/S0104), "net use," and "net session" with [Net](https://attack.mitre.org/software/S0039). In Mac and Linux, [netstat](https://attack.mitre.org/software/S0104) and `lsof` can be used to list current connections. `who -a` and `w` can be used to show which users are currently logged in, similar to "net session". Additionally, built-in features native to network devices and [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) may be used (e.g. `show ip sockets`, `show tcp brief`).(Citation: US-CERT-TA18-106A)

Domain-Name

Value
cancelation.one
simonoo.com
sellscentre.com
minaato.com
olimobile.com

StixFile

Value
83f0f1b491fa83d72a819e3de69455a0b20c6cb48480bcd8cc9c64dbbbc1b581

External References

- https://otx.alienvault.com/pulse/64b0196a91718cb2daa72a1e
- https://cybersecurity.att.com/blogs/security-essentials/stories-from-the-soc-onenote-malspam-detection-response