Jun 23 2023

NETMANAGEIT

Intelligence Report

Bluenoroff's RustBucket campaign

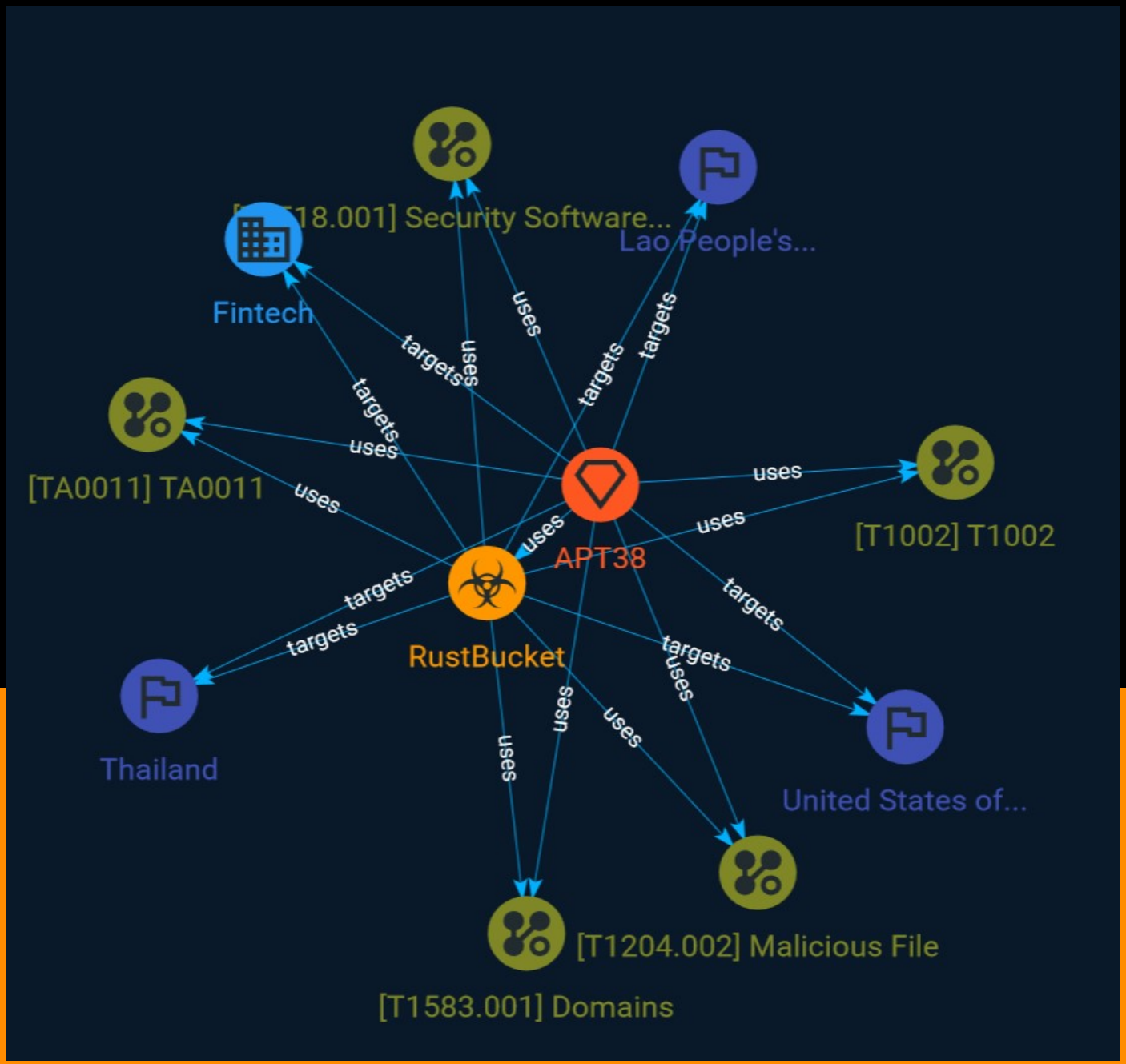

Table of contents

Overview

Entities

External References

Overview

Description

Researchers at Sekoia have investigated Bluenoroff's infrastructure and share their findings in this report.

Confidence

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

15 / 100

Attack-Pattern

Name

Security Software Discovery

ID

T1518.001

Description

Adversaries may attempt to get a listing of security software, configurations, defensive tools, and sensors that are installed on a system or in a cloud environment. This may include things such as firewall rules and anti-virus. Adversaries may use the information from [Security Software Discovery](https://attack.mitre.org/techniques/T1518/001) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Example commands that can be used to obtain security software information are [netsh](https://attack.mitre.org/software/S0108), `reg query` with [Reg](https://attack.mitre.org/software/S0075), `dir` with [cmd](https://attack.mitre.org/software/S0106), and [Tasklist](https://attack.mitre.org/software/S0057), but other indicators of discovery behavior may be more specific to the type of software or security system the adversary is looking for. It is becoming more common to see macOS malware perform checks for LittleSnitch and KnockKnock software. Adversaries may also utilize cloud APIs to discover the configurations of firewall rules within an environment.(Citation: Expel IO Evil in AWS) For example, the permitted IP ranges, ports or user accounts for the inbound/outbound rules of security groups, virtual firewalls established within AWS for EC2 and/or VPC instances, can be revealed by the `DescribeSecurityGroups` action with various request parameters. (Citation: DescribeSecurityGroups - Amazon Elastic Compute Cloud)

Name

Malicious File

ID

T1204.002

Description

An adversary may rely upon a user opening a malicious file in order to gain execution. Users may be subjected to social engineering to get them to open a file that will lead to code execution. This user action will typically be observed as follow-on behavior from [Spearphishing Attachment](https://attack.mitre.org/techniques/T1566/001). Adversaries may use several types of files that require a user to execute them, including .doc, .pdf, .xls, .rtf, .scr, .exe, .lnk, .pif, and .cpl. Adversaries may employ various forms of [Masquerading](https://attack.mitre.org/techniques/T1036) and [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to increase the likelihood that a user will open and successfully execute a malicious file. These methods may include using a familiar naming convention and/or password protecting the file and supplying instructions to a user on how to open it.(Citation: Password Protected Word Docs) While [Malicious File](https://attack.mitre.org/techniques/T1204/002) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534).

Name

TA0011

ID

TA0011

Name

T1002

ID

T1002

Name

Domains

ID

T1583.001

Description

Adversaries may acquire domains that can be used during targeting. Domain names are the human readable names used to represent one or more IP addresses. They can be purchased or, in some cases, acquired for free. Adversaries may use acquired domains for a variety of purposes, including for [Phishing](https://attack.mitre.org/techniques/T1566), [Drive-by Compromise](https://attack.mitre.org/techniques/T1189), and Command and Control.(Citation: CISA MSS Sep 2020) Adversaries may choose domains that are similar to legitimate domains, including through use of homoglyphs or use of a different top-level domain (TLD).(Citation: FireEye APT28)(Citation: PaypalScam) Typosquatting may be used to aid in delivery of payloads via [Drive-by Compromise](https://attack.mitre.org/techniques/T1189). Adversaries may also use internationalized domain names (IDNs) and different character sets (e.g. Cyrillic, Greek, etc.) to execute "IDN homograph attacks," creating visually similar lookalike domains used to deliver malware to victim machines.(Citation: CISA IDN ST05-016)(Citation: tt_httrack_fake_domains)(Citation: tt_obliqueRAT)(Citation: httrack_unhcr)(Citation: lazgroup_idn_phishing) Adversaries may also acquire and repurpose expired domains, which may be potentially already allowlisted/trusted by defenders based on an existing reputation/history.(Citation: Categorisation_not_boundary)(Citation: Domain_Steal_CC)(Citation: Redirectors_Domain_Fronting)(Citation: bypass_webproxy_filtering) Domain registrars each maintain a publicly viewable database that displays contact information for every registered domain. Private WHOIS services display alternative information, such as their own company data, rather than the owner of the domain. Adversaries may use such private WHOIS services to obscure information about who owns a purchased domain. Adversaries may further interrupt efforts to track their infrastructure by using varied registration information and purchasing domains with different domain registrars.(Citation: Mandiant APT1)

Sector

Name
Fintech

Intrusion-Set

Name

APT38

Description

[APT38](https://attack.mitre.org/groups/G0082) is a North Korean state-sponsored threat group that specializes in financial cyber operations; it has been attributed to the Reconnaissance General Bureau.(Citation: CISA AA20-239A BeagleBoyz August 2020) Active since at least 2014, [APT38](https://attack.mitre.org/groups/G0082) has targeted banks, financial institutions, casinos, cryptocurrency exchanges, SWIFT system endpoints, and ATMs in at least 38 countries worldwide. Significant operations include the 2016 Bank of Bangladesh heist, during which [APT38](https://attack.mitre.org/groups/G0082) stole $81 million, as well as attacks against Bancomext (2018) and Banco de Chile (2018); some of their attacks have been destructive.(Citation: CISA AA20-239A BeagleBoyz August 2020) (Citation: FireEye APT38 Oct 2018)(Citation: DOJ North Korea Indictment Feb 2021)(Citation: Kaspersky Lazarus Under The Hood Blog 2017) North Korean group definitions are known to have significant overlap, and some security researchers report all North Korean state-sponsored cyber activity under the name [Lazarus Group](https://attack.mitre.org/groups/G0032) instead of tracking clusters or subgroups.

Country

Name
United States of America
Name
Thailand
Name
Lao People's Democratic Republic

Malware

Name
RustBucket

External References

- https://otx.alienvault.com/pulse/646b86330f5e0a80621931b7
- https://blog.sekoia.io/bluenoroffs-rustbucket-campaign