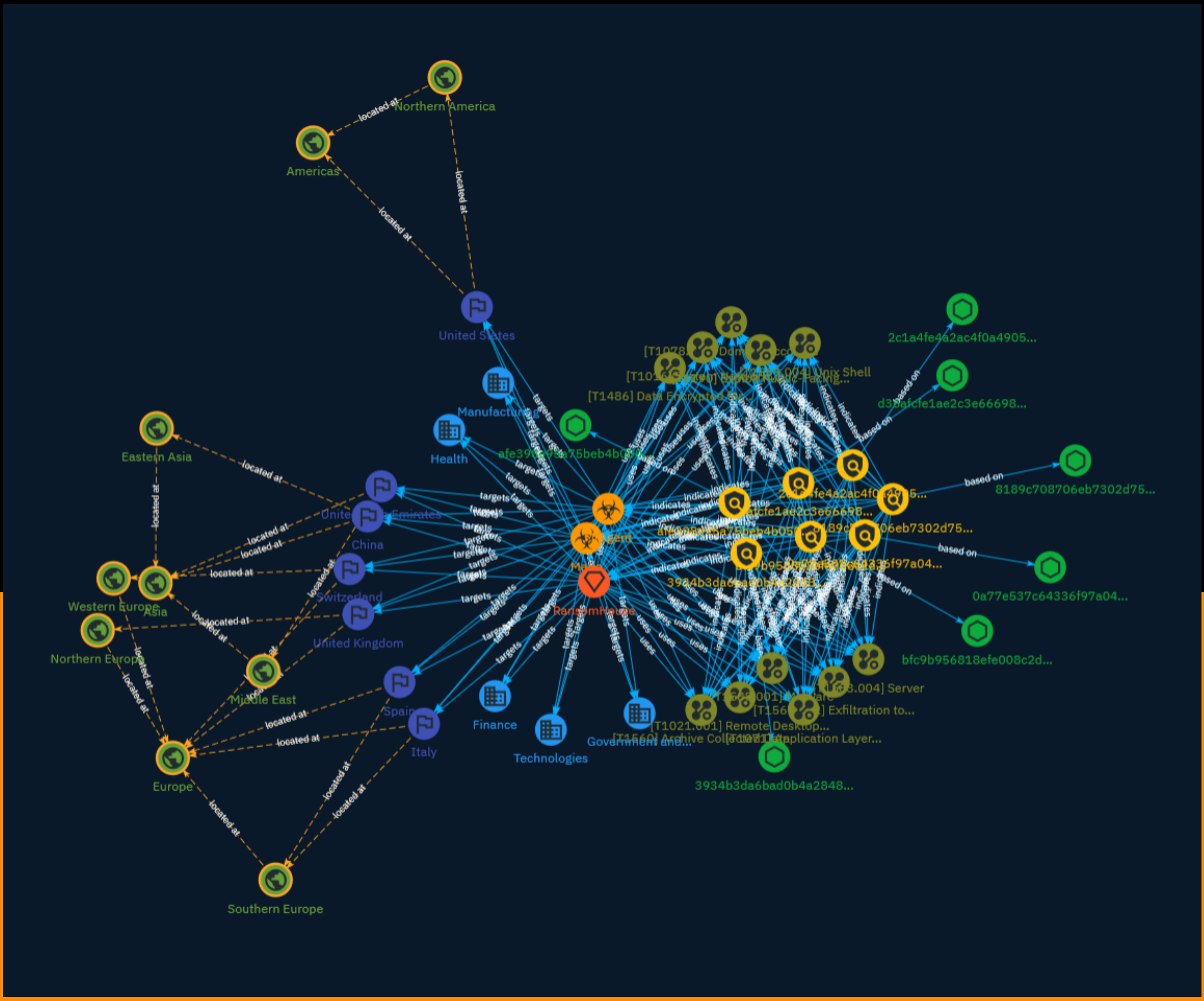
Feb 20 2024

NETMANAGEIT

# Intelligence Report

# RansomHouse am See



# Table of contents

## Overview

## Entities

## Observables

## External References

# Overview

## Description

The RansomHouse group (RaaS) emerged in late 2021 and has been active in deploying ransomware variants to exploit corporate networks. The group extorts its victims twice, first by encrypting their files and demanding a ransom, and second by naming and shaming non-paying victims on their blog, along with which they publish the stolen data from the victim. The group tries to differentiate itself from typical ransomware operators by cultivating an image of a "professional mediator community". This group is identified for using a unique ransomware variant, dubbed Mario ESXi, along with MrAgent, to target both Windows and Linux-based systems. The ransomware shares code with Babuk.

## Confidence

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

15 / 100

# Content

N/A

# Indicator

**Name**

d36afcfe1ae2c3e6669878e6f9310a04fb6c8af525d17c4ffa8b510459d7dd4d

**Description**

is__elf

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'd36afcfe1ae2c3e6669878e6f9310a04fb6c8af525d17c4ffa8b510459d7dd4d']

**Name**

bfc9b956818efe008c2dbf621244b6dc3de8319e89b9fa83c9e412ce70f82f2c

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'bfc9b956818efe008c2dbf621244b6dc3de8319e89b9fa83c9e412ce70f82f2c']

**Name**

afe398e95a75beb4b0508c1bbf7268e8607d03776af0b68386d1e2058b374501

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'afe398e95a75beb4b0508c1bbf7268e8607d03776af0b68386d1e2058b374501']

**Name**

8189c708706eb7302d7598aeee8cd6bdb048bf1a6dbe29c59e50f0a39fd53973

**Description**

is__elf

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '8189c708706eb7302d7598aeee8cd6bdb048bf1a6dbe29c59e50f0a39fd53973']

**Name**

3934b3da6bad0b4a28483e25e7bab919d7ed31f2f51cca22c56535b9f8183a0e

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' =
'3934b3da6bad0b4a28483e25e7bab919d7ed31f2f51cca22c56535b9f8183a0e']

**Name**

2c1a4fe4a2ac4f0a49052f9521458136eb477fe23665dc4b7076fbd32de3005d

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' =
'2c1a4fe4a2ac4f0a49052f9521458136eb477fe23665dc4b7076fbd32de3005d']

**Name**

0a77e537c64336f97a04020e59d17d09d459d1626a075878e2b796d1e1033038

**Pattern Type**

stix

**Pattern**

```
[file:hashes.'SHA-256' =
'0a77e537c64336f97a04020e59d17d09d459d1626a075878e2b796d1e1033038']
```

# Malware

| Name |
|---|
| Mario |

| Name |
|---|
| MrAgent |

# Intrusion-Set

| Name |
|---|
| RansomHouse |

# Attack-Pattern

| Name |
|---|
| Remote Desktop Protocol |
| **ID** |
| T1021.001 |
| **Description** |
| Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to log into a computer using the Remote Desktop Protocol (RDP). The adversary may then perform actions as the logged-on user. Remote desktop is a common feature in operating systems. It allows a user to log into an interactive session with a system desktop graphical user interface on a remote system. Microsoft refers to its implementation of the Remote Desktop Protocol (RDP) as Remote Desktop Services (RDS).(Citation: TechNet Remote Desktop Services) Adversaries may connect to a remote system over RDP/RDS to expand access if the service is enabled and allows access to accounts with known credentials. Adversaries will likely use Credential Access techniques to acquire credentials to use with RDP. Adversaries may also use RDP in conjunction with the [Accessibility Features](https://attack.mitre.org/techniques/T1546/008) or [Terminal Services DLL](https://attack.mitre.org/techniques/T1505/005) for Persistence.(Citation: Alperovitch Malware) |
| **Name** |
| Domain Accounts |
| **ID** |

T1078.002

**Description**

Adversaries may obtain and abuse credentials of a domain account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion.(Citation: TechNet Credential Theft) Domain accounts are those managed by Active Directory Domain Services where access and permissions are configured across systems and services that are part of that domain. Domain accounts can cover users, administrators, and services.(Citation: Microsoft AD Accounts) Adversaries may compromise domain accounts, some with a high level of privileges, through various means such as [OS Credential Dumping](https://attack.mitre.org/techniques/T1003) or password reuse, allowing access to privileged resources of the domain.

**Name**

Exfiltration to Cloud Storage

**ID**

T1567.002

**Description**

Adversaries may exfiltrate data to a cloud storage service rather than over their primary command and control channel. Cloud storage services allow for the storage, edit, and retrieval of data from a remote cloud storage server over the Internet. Examples of cloud storage services include Dropbox and Google Docs. Exfiltration to these cloud storage services can provide a significant amount of cover to the adversary if hosts within the network are already communicating with the service.

**Name**

Data Encrypted for Impact

**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

Unix Shell

## ID

T1059.004

| **Description** |
|---|
| Adversaries may abuse Unix shell commands and scripts for execution. Unix shells are the primary command prompt on Linux and macOS systems, though many variations of the Unix shell exist (e.g. sh, bash, zsh, etc.) depending on the specific OS or distribution. (Citation: DieNet Bash)(Citation: Apple ZShell) Unix shells can control every aspect of a system, with certain commands requiring elevated privileges. Unix shells also support scripts that enable sequential execution of commands as well as other typical programming operations such as conditionals and loops. Common uses of shell scripts include long or repetitive tasks, or the need to run the same set of commands on multiple systems. Adversaries may abuse Unix shells to execute various commands or payloads. Interactive shells may be accessed through command and control channels or during lateral movement such as with [SSH](https://attack.mitre.org/techniques/T1021/004). Adversaries may also leverage shell scripts to deliver and execute multiple commands on victims or as part of payloads used for persistence. |
| **Name** |
| Malware |
| **ID** |
| T1588.001 |
| **Description** |
| Adversaries may buy, steal, or download malware that can be used during targeting. Malicious software can include payloads, droppers, post-compromise tools, backdoors, packers, and C2 protocols. Adversaries may acquire malware to support their operations, obtaining a means for maintaining control of remote machines, evading defenses, and executing post-compromise behaviors. In addition to downloading free malware from the internet, adversaries may purchase these capabilities from third-party entities. Third-party entities can include technology companies that specialize in malware development, criminal marketplaces (including Malware-as-a-Service, or MaaS), or from individuals. In addition to purchasing malware, adversaries may steal and repurpose malware from third-party entities (including other adversaries). |
| **Name** |

System Network Configuration Discovery

**ID**

T1016

**Description**

Adversaries may look for details about the network configuration and settings, such as IP and/or MAC addresses, of systems they access or through information discovery of remote systems. Several operating system administration utilities exist that can be used to gather this information. Examples include [Arp](https://attack.mitre.org/software/S0099), [ipconfig](https://attack.mitre.org/software/S0100)/[ifconfig](https://attack.mitre.org/software/S0101), [nbtstat](https://attack.mitre.org/software/S0102), and [route](https://attack.mitre.org/software/S0103). Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather information about configurations and settings, such as IP addresses of configured interfaces and static/dynamic routes (e.g. `show ip route`, `show ip interface`).(Citation: US-CERT-TA18-106A)(Citation: Mandiant APT41 Global Intrusion ) Adversaries may use the information from [System Network Configuration Discovery](https://attack.mitre.org/techniques/T1016) during automated discovery to shape follow-on behaviors, including determining certain access within the target network and what actions to do next.

**Name**

Server

**ID**

T1583.004

**Description**

Adversaries may buy, lease, or rent physical servers that can be used during targeting. Use of servers allows an adversary to stage, launch, and execute an operation. During post-compromise activity, adversaries may utilize servers for various tasks, including for Command and Control. Adversaries may use web servers to support support watering hole operations, as in [Drive-by Compromise](https://attack.mitre.org/techniques/T1189), or email servers to support [Phishing](https://attack.mitre.org/techniques/T1566) operations. Instead of compromising a third-party [Server](https://attack.mitre.org/techniques/T1584/004) or renting a [Virtual Private Server](https://attack.mitre.org/techniques/T1583/003), adversaries may opt to configure and run their own servers in support of operations. Adversaries may only need a lightweight setup if most of their activities will take place using online infrastructure. Or, they may need to build extensive infrastructure if they want to test, communicate, and control other aspects of their activities on their own systems.(Citation: NYTStuxnet)

**Name**

Archive Collected Data

**ID**

T1560

**Description**

An adversary may compress and/or encrypt data that is collected prior to exfiltration. Compressing the data can help to obfuscate the collected data and minimize the amount of data sent over the network. Encryption can be used to hide information that is being exfiltrated from detection or make exfiltration less conspicuous upon inspection by a defender. Both compression and encryption are done prior to exfiltration, and can be performed using a utility, 3rd party library, or custom method.

**Name**

Exploit Public-Facing Application

**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)

**Name**

Application Layer Protocol

**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.

# Country

| Name |
|---|
| Switzerland |

| Name |
|---|
| Spain |

| Name |
|---|
| Italy |

| Name |
|---|
| United Kingdom |

| Name |
|---|
| United Arab Emirates |

| Name |
|---|
| China |

| Name |
|---|
| United States |

# Region

| Name |
|---|
| Western Europe |

| Name |
|---|
| Southern Europe |

| Name |
|---|
| Northern Europe |

| Name |
|---|
| Europe |

| Name |
|---|
| Middle East |

| Name |
|---|
| Eastern Asia |

| Name |
|---|
| Asia |

| Name |
|---|
| Northern America |

| Name |
|---|
| Americas |

# Sector

| |
|---|
| **Name** |
| Manufacturing |
| **Description** |
| Private entities transforming and selling goods, products and equipment which are not included in other activity sectors. |
| **Name** |
| Technologies |
| **Description** |
| Private entities related to the research, development, manufacturing and distribution of electronics, softwares, computers and products related to information technologies. |
| **Name** |
| Health |
| **Description** |
| Public and private entities involved in research, services and manufacturing activities related to public health. |

| Name |
|---|
| Government and administrations |

| Description |
|---|
| Civilian government institutions and administrations of the executive and legislative branches. The diplomatic and judicial branches are not included. |

| Name |
|---|
| Finance |

| Description |
|---|
| Public and private entities involved in the allocation of assets and liabilities over space and time. |

# StixFile

| Value |
|---|
| d36afcfe1ae2c3e6669878e6f9310a04fb6c8af525d17c4ffa8b510459d7dd4d |
| bfc9b956818efe008c2dbf621244b6dc3de8319e89b9fa83c9e412ce70f82f2c |
| afe398e95a75beb4b0508c1bbf7268e8607d03776af0b68386d1e2058b374501 |
| 8189c708706eb7302d7598aeee8cd6bdb048bf1a6dbe29c59e50f0a39fd53973 |
| 3934b3da6bad0b4a28483e25e7bab919d7ed31f2f51cca22c56535b9f8183a0e |
| 2c1a4fe4a2ac4f0a49052f9521458136eb477fe23665dc4b7076fbd32de3005d |
| 0a77e537c64336f97a04020e59d17d09d459d1626a075878e2b796d1e1033038 |

# External References

- https://www.trellix.com/blogs/research/ransomhouse-am-see/
- https://otx.alienvault.com/pulse/65d365ead2870c71ead3f4c7