The Ransomware Threat Intelligence Center

news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/

Tilly Travers March 17, 2022

Introduction

The ransomware landscape is a complex, crowded and rapidly evolving ecosystem. New and rebranded groups appear and disappear continuously, while the operators behind them share, rent, steal, or copy each other's attack tools, playbooks and even infrastructure.

Sophos has been monitoring and reporting on the ransomware landscape for years, building an unrivalled library of insight and analysis. The **Ransomware Threat Intelligence Center** brings together a curated list of the most important research articles and reports published by Sophos on prevalent, new, and emerging ransomware threats, including their tools, techniques, and behaviors, from 2018 to the present. The content will be updated regularly as new material becomes available.

For further information on ransomware, including advice on security best practice and the latest State of Ransomware report, visit Sophos' Resources to Stop Ransomware.

Sophos Research and Reports on Prevalent and New Ransomware Groups, 2018 to 2022

Astro Locker

Sophos MTR in real time: What is Astro Locker team?

March 31, 2021 – A Sophos incident response investigation uncovers similarities between Astro Locker and Mount Locker ransomware

Avos Locker

Avos Locker remotely accesses boxes, even running in Safe Mode

Dec. 22, 2021 – Sophos reports how the relatively new ransomware-as-a-service (RaaS), Avos Locker boots target computers into Safe Mode to execute the ransomware and tries to disable security software

Atom Silo

Atom Silo ransomware actors use Confluence exploit, DLL side-load for stealthy attack

Oct. 4, 2021 – Sophos reports on an attack by the relatively new ransomware group Atom Silo that leveraged a recent vulnerability in Atlassian's Confluence collaboration software and tried to disrupt endpoint protection software. The Confluence vulnerability was also exploited by a crypto miner

Avaddon

What to expect when you've been hit with Avaddon ransomware

May 24, 2021 – Part of a series designed to help IT administrators facing the impact of an attack involving a particular ransomware family

Black Kingdom

Black Kingdom ransomware begins appearing on Exchange servers

March 23, 2021 – Sophos reports on a novel, if fairly basic ransomware targeting Microsoft Exchange servers that haven't been patched against the ProxyLogon exploit

BlackMatter

BlackMatter ransomware emerges from the shadow of DarkSide

Aug. 9, 2021 – Sophos reports on a new RaaS that calls itself BlackMatter and adopts tools and techniques from REvil, DarkSide and LockBit 2.0

Conti

Sophos has reported extensively on the prolific Conti RaaS operation. Researchers will continue to track the evolution of this high profile threat following the events of early March 2022, when Conti's stance on the Russia Ukraine war led to a series of public leaks of its attack playbook, toolset, internal communications, source code and more.

Sophos analysis and insight on Conti ransomware include:

What to expect when you've been hit with Conti ransomware

Feb. 16, 2021 – Part of a series designed to help IT administrators facing the impact of an attack involving a particular ransomware family

Conti ransomware: Evasive by nature

Feb. 16, 2021 – Sophos reports on how the attackers spreading Conti have switched gears to a completely fileless attack method

A Conti ransomware attack day-by-day

Feb. 16, 2021 – Sophos reports on the unfolding of a Conti ransomware incident

Conti affiliates use ProxyShell Exchange exploit in ransomware attacks

Sep. 3, 2021 – Sophos reports on an investigation into a Conti ransomware attack where the attackers used a ProxyShell exploit

Cring

Cring ransomware group exploits ancient ColdFusion server

Sep. 21, 2021 – Sophos reports on an unknown threat actor exploiting a vulnerability in an 11-year-old installation of Adobe ColdFusion 9 and deploying rarely seen Cring ransomware

DearCry

DearCry ransomware attacks exploit Exchange server vulnerabilities

March15, 2021 – Sophos reports on an unsophisticated, "beginner" ransomware called DearCry, which mimics the notorious WannaCry ransomware

Dharma

Color by numbers: inside a Dharma ransomware-as-a-service attack

Aug.12, 2020 – Sophos reports on the Dharma RaaS that targets smaller businesses and provides affiliates with detailed, step-by-step attack scripts

DarkSide

A defender's view inside a DarkSide ransomware attack

May 11, 2021 – A Sophos deep dive into the attack methods of the DarkSide ransomware group

Egregor

Egregor ransomware: Maze's heir apparent

Dec. 8, 2020 – Sophos reports on a new RaaS variant of Sekhmet ransomware that appears to have picked up where Maze left off

Entropy

Dridex bots deliver Entropy ransomware in recent attacks

Feb. 23, 2022 – Sophos reports on how code used in Entropy ransomware bears a resemblance to code used in Dridex malware, suggesting a possible common origin

Epsilon Red

A new ransomware enters the fray: Epsilon Red

May 28, 2021 – Sophos reports on a new, bare-bones ransomware that offloads most of its functionality to a series of PowerShell scripts

GandCrab

GandCrab 101: All about the most widely distributed ransomware of the moment

March 5, 2019 – A deep dive into a ransomware that dominated the landscape in 2019

Directed attacks against MySQL servers deliver ransomware

May 24, 2019 – Sophos reports on an unknown adversary attacking internet-facing Windows database servers with GandCrab ransomware

LockBit

LockBit ransomware borrows tricks to keep up with REvil and Maze

April 24, 2020 – Sophos reports on how LockBit is implementing techniques and behaviors from other high profile ransomware groups

LockBit uses automated attack tools to identify tasty targets

Oct. 21, 2021 – Sophos reports on how the operators behind LockBit ransomware are using renamed copies of PowerShell and other automated tools to searched for systems with valuable data

Attackers linger on government agency computers before deploying LockBit ransomware

April 12, 2022 – Sophos reports on how attackers breached and then spent five months in a compromised network, Googling for tools to further their attack before exfiltrating data and deploying LockBit ransomware

LockFile

LockFile ransomware's box of tricks: intermittent encryption and evasion

Aug. 27, 2021 – Sophos discovers a new ransomware family leveraging ProxyShell and using intermittent encryption of files to evade detection by anti-ransomware tools

Matrix

Matrix: Targeted, small scale, canary in the coalmine ransomware

Jan. 30, 2019 – Sophos reports on how the unsophisticated Matrix ransomware succeeds by leveraging vulnerable remote desktops to breach networks and disrupt targets

Maze

Maze ransomware: extorting victims for 1 year and counting

May 12, 2020 – Sophos reports on how the Maze ransomware operators were one of the first ransomware operations to use data theft as a way of coercing victims to pay the ransom demand

Maze attackers adopt Ragnar Locker virtual machine technique

Sep. 17, 2020 – Sophos reports on how Maze operators adopted a cumbersome ransomware delivery technique from Ragnar Locker after several failed attempts to deploy the ransomware

MTR Casebook: Blocking a $15 million Maze ransomware attack

Sep. 22, 2020 – A day-by-day account of the unfolding of a major Maze ransomware attack

MegaCortex

"MegaCortex" ransomware wants to be The One

May 3, 2019 – Sophos reports on a new, sophisticated ransomware group leveraging both automated and manual components

MegaCortex, deconstructed: mysteries mount as analysis continues

May 10, 2019 – A follow on research article including new insight on the ransomware group's tools, techniques, and misdirection tactics

Memento

New ransomware actor uses password protected archives to bypass encryption protection

Nov. 18, 2021 – Sophos reports on an incident involving the new ransomware group, Memento, that failed to encrypt files so instead copied them into password-protected archives

Midas

Windows services lay the groundwork for a Midas ransomware attack

Jan. 25, 2022 – Sophos reports on a ransomware attack that made extensive use of vulnerable remote access services and PowerShell scripts

Nefilim

Nefilim Ransomware Attack Uses “Ghost” Credentials

Jan. 26, 202 – Sophos reports on an incident where the attackers gained access to the target using the account credentials of a deceased employee

Netwalker

Netwalker ransomware tools give insight into threat actor

May 27, 2020 – Sophos details the tactics, techniques, and procedures (TTPs) used by Netwalker after discovering a trove of malware and related files

ProLock

ProLock ransomware gives you the first 8 kilobytes of decryption for free

July 27, 2020 – Sophos reports on the attack chain and TTPs of this new ransomware

Python

Python ransomware script targets ESXi server for encryption

Oct. 5, 2021 – Sophos reports one of the fastest ransomware attacks it has seen, where a Python script on the target’s virtual machine hypervisor encrypted all virtual disks

RagnarLocker

Ragnar Locker ransomware deploys virtual machine to dodge security

May 21, 2020 – Sophos reports on an incident where the attackers deployed a full virtual machine on each targeted device to hide the ransomware from view

Ragnarok

Asnarök attackers twice modified attack midstream

May 21, 2021 – Sophos reports on how Asnarok attackers try to deploy Ragnarok ransomware through an unpatched firewall

REvil

Relentless REvil, revealed: RaaS as variable as the criminals who use it

June 11, 2021 – Sophos details the different TTPs seen among the affiliate customers of the REvil RaaS

What to expect when you've been hit with REvil ransomware

June 30, 2021 – Part of a series designed to help IT administrators facing the impact of an attack involving a particular ransomware family

Independence Day: REvil uses supply chain exploit to attack hundreds of businesses

July 4, 2021 – Sophos details the crypto-extortion attack launched by a REvil affiliate using a malicious update to exploit Kaseya's VSA remote management service

RobbinHood

Living off another land: Ransomware borrows vulnerable driver to remove security software

Feb. 6, 2020 – Sophos reports on attacks where attackers deployed a legitimate, digitally signed hardware driver to delete security products from targeted computers before deploying RobbinHood ransomware

Ryuk

They're back: inside a new Ryuk ransomware attack

Oct. 14, 2020 – Sophos reports on the return of Ryuk after a period of quiet, with evolved tools for compromise and ransomware deployment

MTR in Real Time: Pirates pave way for Ryuk ransomware

May 6, 2021 – Sophos reports on an incident where downloading a pirate software program led attackers to breach the network of a research institute and deploy Ryuk ransomware

SamSam

Sophos releases SamSam ransomware report

July 31, 2018 – Sophos releases a deep dive into SamSam ransomware

How a SamSam-like attack happens, and what you can do about it

Nov. 29, 2018 – Sophos details a typical SamSam ransomware attack and how to defend against it

Snatch

Snatch ransomware reboots PCs into Safe Mode to bypass protection

Dec. 9, 2019 – Sophos reports on a novel hybrid data theft-ransomware threat that disables security protections by rebooting Windows machines mid-attack

WannaCry

The WannaCry hangover

Sep. 16, 2019 – Sophos reports how, more than two years on, modified WannaCry variants still cause headaches for IT admins and security analysts

WastedLocker

WastedLocker's techniques point to a familiar heritage

Aug. 4, 2020 – Sophos reports on how WastedLocker evades detection by performing most operations in memory, and shares several characteristics with the Bitpaymer ransomware family

Additional Assets

Collective Reports and Analyses

How ransomware attacks: What defenders should know about the most prevalent and persistent ransomware families

The Active Adversary Playbook 2021

The Sophos 2019 Threat Report

The Sophos 2020 Threat Report

The Sophos 2021 Threat Report

The Sophos 2022 Threat Report

Insight and Advisory Articles

How the most damaging ransomware evades IT security

The realities of ransomware: Five signs you're about to be attacked

The realities of ransomware: Extortion goes social in 2020

The realities of ransomware: Why it's not just a passing fad

The realities of ransomware: A victim's eye view of an attack

The realities of ransomware: The evasion arms race

Winners and losers in the ransomware turf wars

The top 10 ways ransomware operators ramp up the pressure to pay

Ransomware mishaps: Adversaries have their off days too