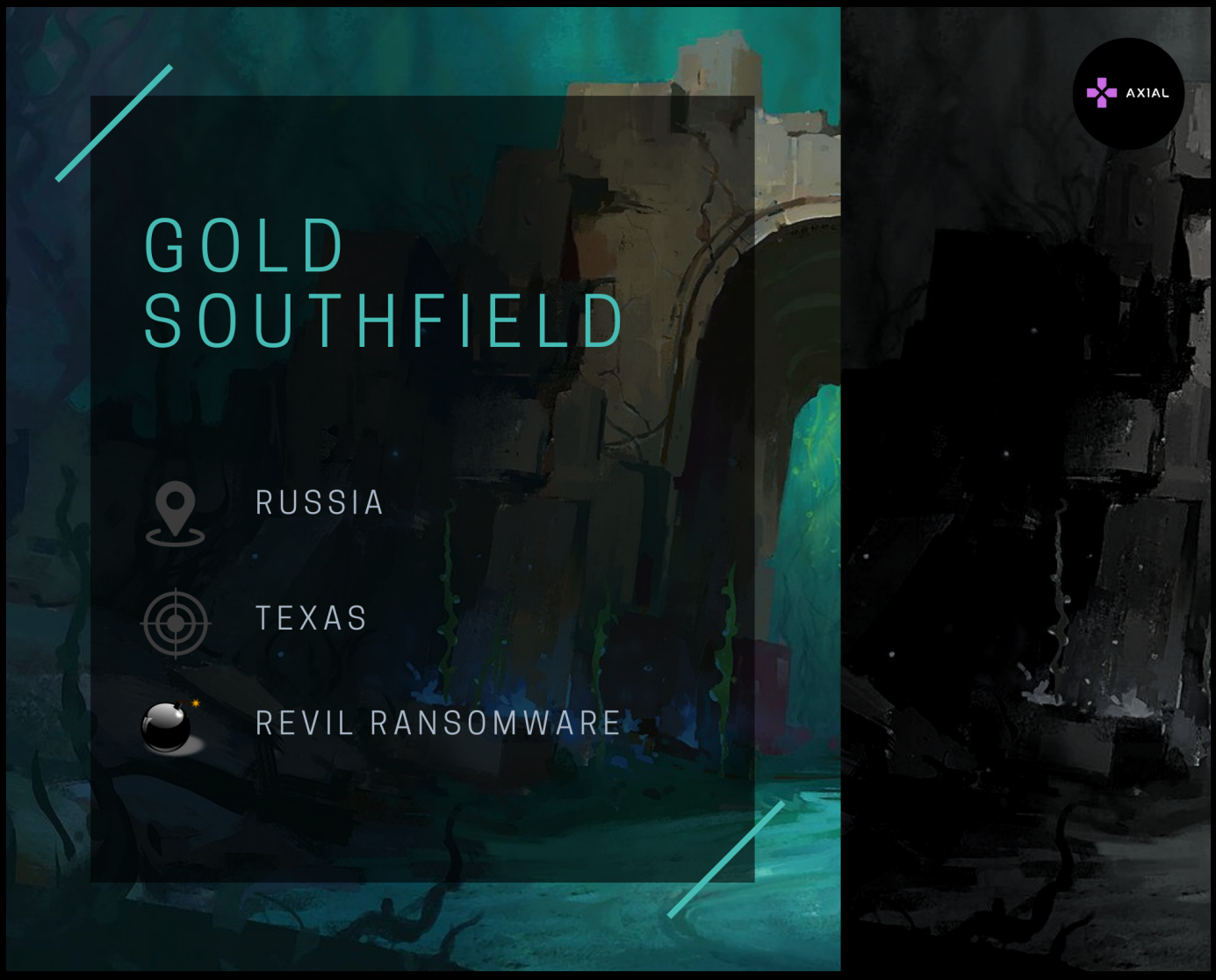
GOLD SOUTHFIELD



HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON GOLD SOUTHFIELD : ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

GOLD SOUTHFIELD is a financially motivated cybercriminal threat group that authors and operates the REvil (aka Sodinokibi) ransomware on behalf of various affiliated threat groups. Operational since April 2019, the group obtained the GandCrab source code from GOLD GARDEN, the operators of GandCrab that voluntarily withdrew their ransomware from underground markets in May 2019. GOLD SOUTHFIELD is responsible for authoring REvil and operating the backend infrastructure used by affiliates (also called partners) to create malware builds and to collect ransom payments from victims. CTU researchers assess with high confidence that GOLD SOUTHFIELD is a former GandCrab affiliate and continues to work with other former GandCrab affiliates.

GandCrab and Sodinokibi have been observed to be distributed by DanaBot (operated by Scully Spider, TA547) and Taurus Loader.

II. TARGETS

-Countries: Worldwide.

Pinchy Spider is the criminal group behind the development of the ransomware most commonly known as GandCrab, which has been active since January 2018. Pinchy Spider sells access to use GandCrab ransomware under a partnership program with a limited number of accounts. The program is operated with a 60-40 split in profits (60 percent to the customer), as is common among eCrime actors, but Pinchy Spider is also willing to negotiate up to a 70-30 split for “sophisticated” customers.

III. TOOLS USED

certutil, Cobalt Strike, GandCrab, Sodinokibi.

AX1AL

IV. CAMPAIGNS

Apr 2019
Sodinokibi ransomware exploits WebLogic Server vulnerability

Jun 2019
Yesterday night, a source in the malware community has told ZDNet that the GandCrab RaaS operator formally announced plans to shut down their service within a month.The announcement was made in an official thread on a well-known hacking forum, where the GandCrab RaaS has advertised its service since January 2018, when it formally launched.

Aug 2019
Over 20 Texas local governments hit in 'coordinated ransomware attack".

Dec 2019
CyrusOne, one of the biggest data center providers in the US, has suffered a ransomware attack, ZDNet has learned.

Dec 2019
Sodinokibi Ransomware Behind Travelex Fiasco: Report.

Dec 2019
A crypto virus that attacked the Albany County Airport Authority's computer management provider during the Christmas holiday period ended up infecting the authority's servers as well, encrypting files and demanding a ransom payment.

Jan 2020
New Jersey Synagogue Suffers Sodinokibi Ransomware Attack

Jan 2020
Sodinokibi Ransomware Publishes Stolen Data for the First TimeThey claim this data belongs to Artech Information Systems, who describe themselves as a 'minority- and women-owned diversity supplier and one of the largest IT staffing companies in the U.S', and that they will release more if a ransom is not paid.

Feb 2020
The operators of the Sodinokibi Ransomware (REvil) have started urging affiliates to copy their victim's data before encrypting computers so it can be used as leverage on a new data leak site that is being launched soon.

Feb 2020
The operators behind Sodinokibi Ransomware published download links to files containing what they claim is financial and work documents, as well as customers' personal data stolen from giant U.S. fashion house Kenneth Cole Productions.

Mar 2020
The operators of the Sodinokibi Ransomware are threatening to publicly share a company's 'dirty' financial secrets because they refused to pay the demanded ransom.As organizations decide to restore their data manually or via backups instead of paying ransoms, ransomware operators are escalating their attacks.

Mar 2020
Recently, the Sodinokibi Ransomware operators published over 12 GB of stolen data allegedly belonging to a company named Brooks International for not paying the ransom.

IV. CAMPAIGNS

Apr 2020
Sodinokibi Ransomware to stop taking Bitcoin to hide money trail

Apr 2020
SeaChange video platform allegedly hit by Sodinokibi ransomware.

May 2020
REvil ransomware threatens to leak A-list celebrities' legal docs

May 2020
REvil ransomware gang publishes 'Elexon staff's passports' after UK electrical middleman shrugs off attack.

May 2020
Here come REvil ransomware operators with another massive data leak. In this instance, they leaked the confidential data of Agromart Group, well-known crop production partners.

Jun 2020
REvil ransomware creates eBay-like auction site for stolen data.

Jun 2020
REvil ransomware operators have been observed while scanning one of their victim's network for Point of Sale (PoS) servers by researchers with Symantec's Threat Intelligence team.

Jun 2020
The threat actor behind the Sodinokibi (REvil) ransomware is demanding a $14 million ransom from Brazilian-based electrical energy company Light S.A.

Jul 2020
A ransomware gang has infected the internal network of Telecom Argentina, one of the country's largest internet service providers, and is now asking for a $7.5 million ransom demand to unlock encrypted files.

Jul 2020
Administrador de Infraestructuras Ferroviarias (ADIF), a Spanish state-owned railway infrastructure manager was hit by REVil ransomware operators.

Aug 2020
Brown-Forman, one of the largest U.S. companies in the spirits and wine business, suffered a cyber attack. The intruders allegedly copied 1TB of confidential data.

Sep 2020
REvil ransomware deposits $1 million in hacker recruitment drive.

Jul 2020
GandCrab ransomware operator arrested in Belarus

V. REFERENCES

1. https://blog.talosintelligence.com/2019/04/sodinokibi-ransomware-exploits-weblogic.html
2. https://www.crowdstrike.com/blog/pinchy-spider-adopts-big-game-hunting/
3. https://krebsonsecurity.com/2019/07/whos-behind-the-gandcrab-ransomware/
4. https://www.secureworks.com/blog/revil-the-gandcrab-connection
5. https://blog.morphisec.com/threat-profile-gandcrab-ransomware
6. https://www.kpn.com/security-blogs/Tracking-REvil.htm
7. https://www.cybereason.com/blog/the-sodinokibi-ransomware-attack