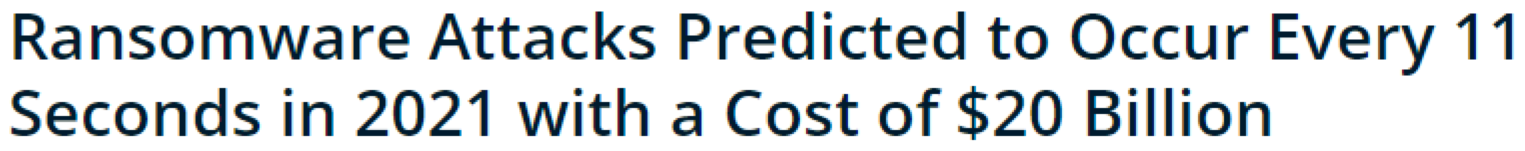
RANSOMWARE : APT'S VS VULNERABILITIES

KAT SYKES - THREAT INTEL

THE PROBLEM

- Ransomware attacks have become synonymous with Advanced Persistent Threat (APT) actors but ransomware at the basic level exploits weaknesses in defenses, namely known (and sometimes undisclosed) vulnerabilities.
- What would happen if the conversation around ransomware changed and instead of focusing on threat actors, companies and security teams were encouraged to focus on the problem, **vulnerabilities**!



Ransomware Attacks Predicted to Occur Every 11 Seconds in 2021 with a Cost of $20 Billion

WHAT IS RANSOMWARE?

- CyberArk Glossary : a type of malware designed to extort victims for financial gain
- Malwarebytes : a type of malware that prevents users from accessing their system or personal files and demands ransom payment in order to regain access.
- Cambridge English Dictionary : software designed by criminals to prevent computer users from getting access to their own computer system or files unless they pay money.

CASE STUDY ONE

Colonial Pipeline

- Attack identified 06 May 2021
- Threat actors gained access to personally identifiable information of 5,810 individuals
- Colonial Pipeline paid the group $4.4 million to regain access

DarkSide

- Operated between 2020 and 2021
- Impacted 47+ organisations
- **Exploited vulnerable Citrix (CVE-2019-19781), Remote Desktop Web, or remote desktop protocol**
- Ransomware-as-a-Service model

CASE STUDY TWO

AXA

- AXA identified a ransomware attack around 17 May impacting their Asia Assistance division
- Threat actors gained access to personally identifiable and medical information
- The requested ransom from AXA wasn't disclosed though asks from Avaddon are between $40,000 and $600,000

Avaddon

- Operated between 2019 and 2021
- Believed to have impacted 2,934 organisations during its lifespan
- **Targeted exposed Remote Desktop Service connections (such as CVE-2019-0708)**
- Ransomware-as-a-Service model

CASE STUDY THREE

Bangkok Air

- Attack identified on 23 August 2021
- Threat actors gained access to personally identifiable and financial information
- Information was disclosed on the groups data leak site when the ransom wasn't paid

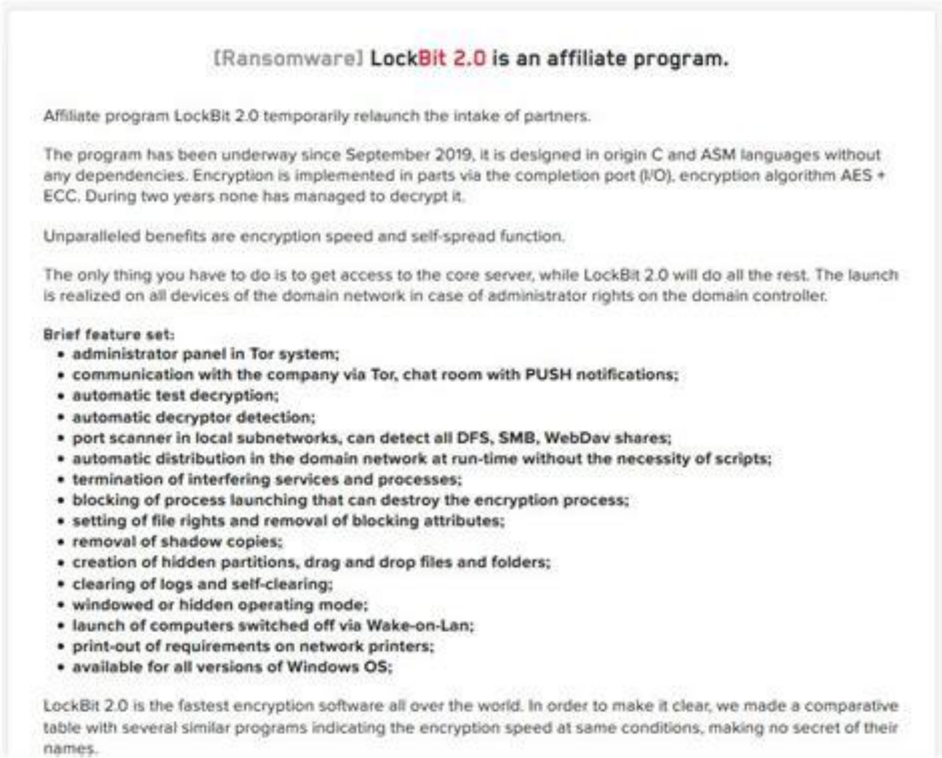
Lockbit 2.0

- Operating since 2019
- Impacted 70+ organisations to date
- **Exploiting vulnerabilities in Fortinet FortiOS and FortiProxy (including CVE-2018-13379)**
- Ransomware-as-a-Service model

WHAT DO THESE ATTACKS HAVE IN COMMON?

Ransomware-as-a-Service (RaaS)

A business model used by ransomware developers, in which they lease variants in the same way that legitimate software developers lease Software-as-a-Service (SaaS) products. RaaS gives everyone, even people without much technical knowledge, the ability to launch ransomware attacks just by signing up for a service.



[Ransomware] LockBit 2.0 is an affiliate program.

Affiliate program LockBit 2.0 temporarily relaunch the intake of partners.

The program has been underway since September 2019, it is designed in origin C and ASM languages without any dependencies. Encryption is implemented in parts via the completion port (I/O), encryption algorithm AES + ECC. During two years none has managed to decrypt it.

Unparalleled benefits are encryption speed and self-spread function.

The only thing you have to do is to get access to the core server, while LockBit 2.0 will do all the rest. The launch is realized on all devices of the domain network in case of administrator rights on the domain controller.

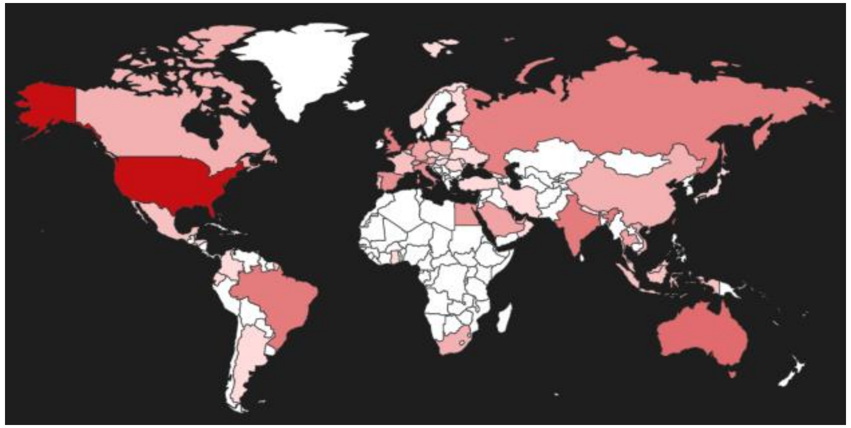
Brief feature set:

- **administrator panel in Tor system;**
- **communication with the company via Tor, chat room with PUSH notifications;**
- **automatic test decryption;**
- **automatic decryptor detection;**
- **port scanner in local subnetworks, can detect all DFS, SMB, WebDav shares;**
- **automatic distribution in the domain network at run-time without the necessity of scripts;**
- **termination of interfering services and processes;**
- **blocking of process launching that can destroy the encryption process;**
- **setting of file rights and removal of blocking attributes;**
- **removal of shadow copies;**
- **creation of hidden partitions, drag and drop files and folders;**
- **clearing of logs and self-clearing;**
- **windowed or hidden operating mode;**
- **launch of computers switched off via Wake-on-Lan;**
- **print-out of requirements on network printers;**
- **available for all versions of Windows OS;**

LockBit 2.0 is the fastest encryption software all over the world. In order to make it clear, we made a comparative table with several similar programs indicating the encryption speed at same conditions, making no secret of their names.

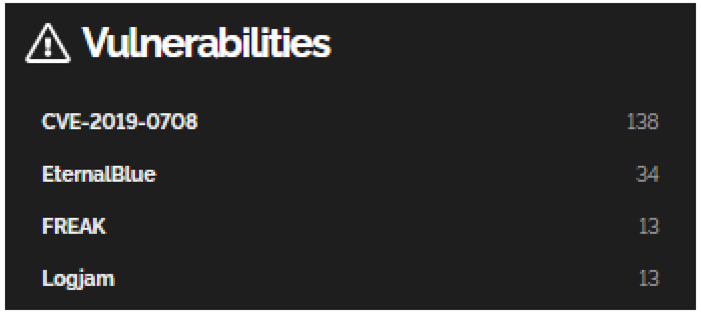
WHAT DO THESE ATTACKS HAVE IN COMMON? 2.0

Citrix



Shodan: Citrix Gateway port:"443"

Windows 7

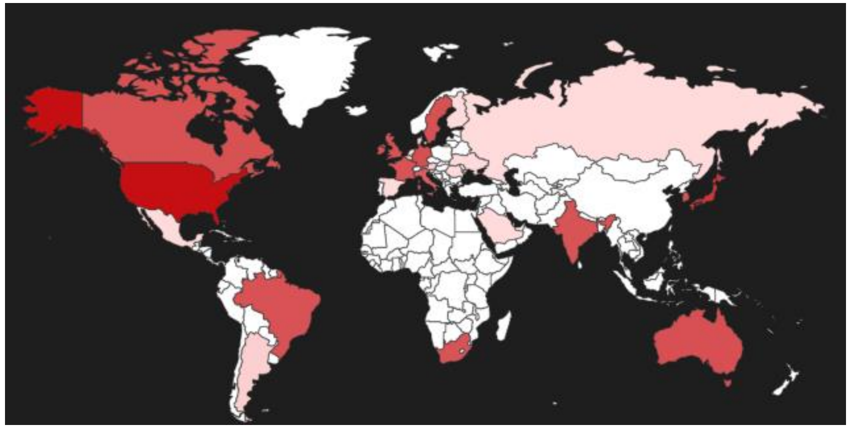


⚠ Vulnerabilities

CVE-2019-0708	138
EternalBlue	34
FREAK	13
Logjam	13

Shodan: Windows 7 country:"GB"

Fortinet

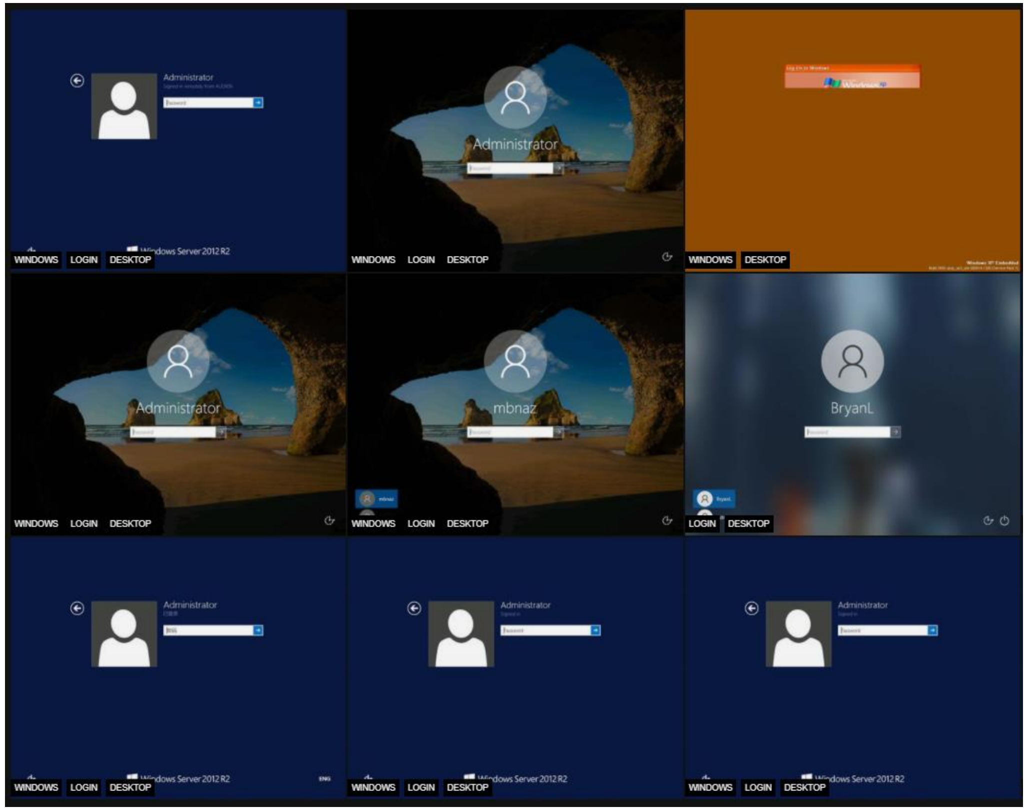


Shodan: Fortinet port:"443"

Identifiable on the Internet

SO, WHAT NEXT?

- The increase of RaaS means that threat actors and affiliates will make a service work for them
- Scanning for vulnerable software and recruitment of Pen Testers likely to continue
- Emisoft advise ransomware attacks cost organisations at least £30 billion in business interruption and ransom payments in 2020



By 2025, organizations will invest more than $1 trillion in their cybersecurity.

SO,WHAT NEXT? 2.0

- **Vulnerability Management Programme / Policies** : A programme that doesn't just focus on published CVE's and the risk score advised but also considers organisational risk, end-of-life software and zero-day vulnerabilities
- **Red Teaming** : Assist in bolstering defenses by simulating real-world attacks by replicating the Techniques, Tactics and Procedures (TTPs) of real-world adversaries including scanning for vulnerable software
- **Social Engineering Awareness Programme** : Security defenses are not infallible, ensure your employees understand what current malicious emails look like and build a culture of personal online security responsibility

THANK YOU FOR LISTENING!