

Ransomware and the Future of Cyberwarfare

Oct 5, 2022



Maggie MacAlpine

Twitter:
[@MaggieMacAlpine](https://twitter.com/MaggieMacAlpine)

Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid. In recent years, ransomware incidents have become increasingly prevalent among the Nation's state, local, tribal, and territorial (SLTT) government entities and critical infrastructure organizations.

Ransomware 101, CISA.gov

The Crisis of Ransomware

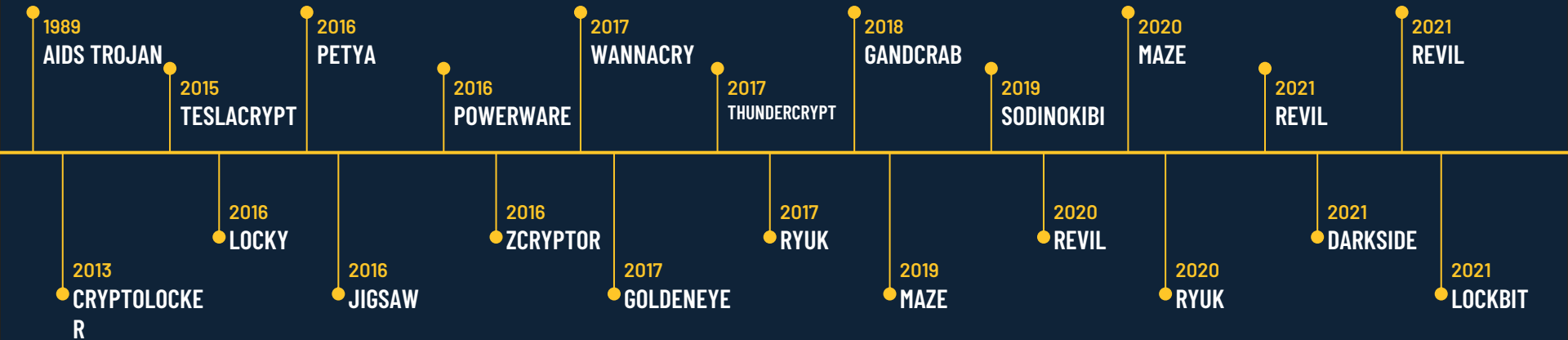
Ransomware is **sophisticated and evolving** faster than traditional prevention measures

Ransomware attacks are **increasing in frequency and severity**

Ransomware-as-a-Service brings **advanced malware to laymen adversaries**

Double and triple extortion **increase the probability of ransom payment**

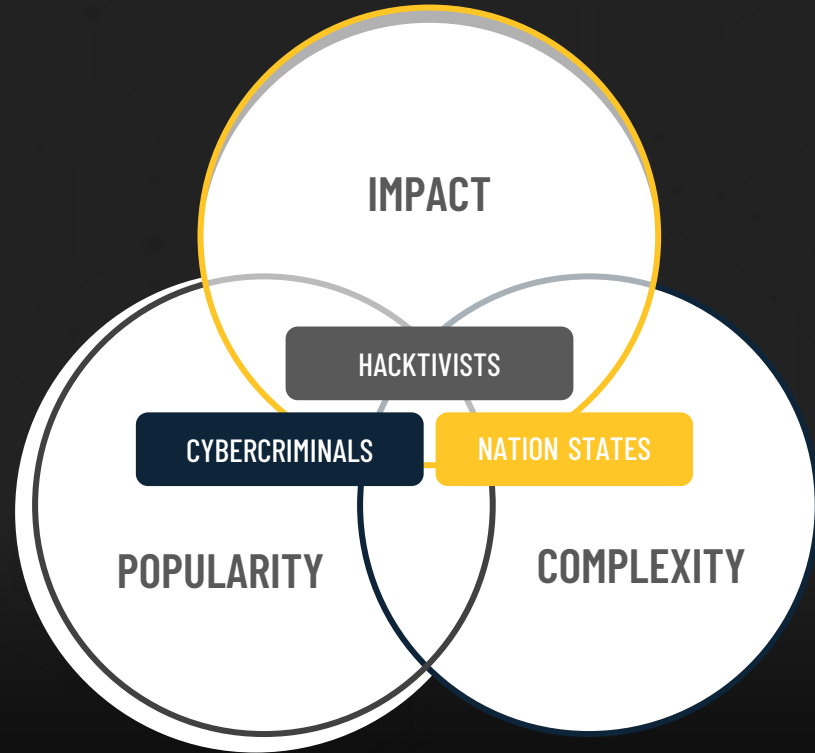
Ransomware **doesn't discriminate** - any organization could be a target



WHY DO ATTACKERS USE RANSOMWARE?

Ransomware:

A type of malware designed to block access to systems or data until a ransom is paid.



The Big Business of Ransomware

There is a massive dark economy that supports ransomware

Ransomware is a mature, mechanized and industrial business

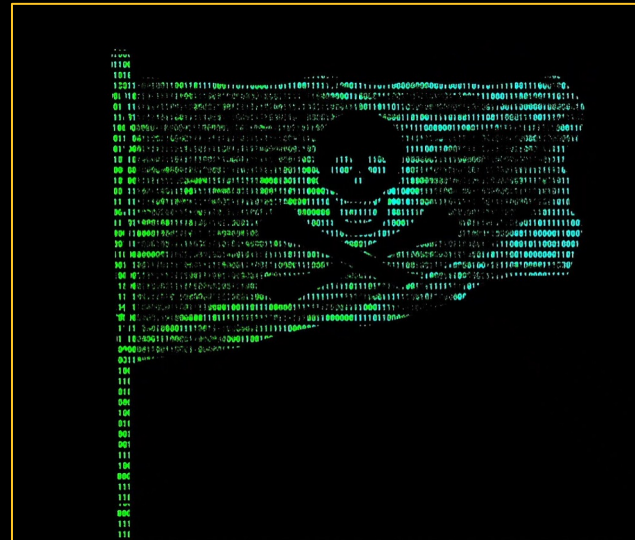
More R&D funding than large legitimate businesses

Mimic legitimate business models, akin to startups

Leverage ML, Cloud Infrastructure, Open-Source Tools

Teams with specialized roles

These are well funded and unprepared InfoSec teams are outmatched



Ransomware Attacks

Impact the Real World

The effects of a ransomware operation are more than just a technical crisis

Colonial Pipeline - May 7, 2021
Restricted oil supply in U.S.

JBS - May 31, 2021
World's largest meat supplier disabled

Springhill Medical Center - 2019
Baby dies due to ransomware attack at hospital

How a major oil pipeline got held for ransom

The largest petroleum pipeline in the country was reportedly breached by a single leaked password.

By Sara Morrison | Updated Jun 8, 2021, 12:50pm EDT

f t SHARE



Colonial Pipeline shut down its massive oil pipeline after a ransomware attack took some of its systems offline. Above, a Colonial facility in 2016. | Luke Sharrett/Bloomberg/Getty Images

NEWS POLITICS COVID-19 U.S. NEWS WORLD OPINION BUSINESS WATCH NOW

NEWS

Baby died because of ransomware attack on hospital, suit says

The filing is the first credible public claim that someone's death was caused at least in part by hackers who remotely shut down a hospital's computers.

Ransomware attack hits another massive, crucial industry: Meat

JBS Foods, the world's largest meat producer, ultimately paid \$11 million in ransom.

By Sara Morrison | Updated Jun 10, 2021, 9:35am EDT

f t SHARE

RANSOMWARE

More of an issue than ever

105%

Increase in ransomware attacks since the start of the COVID-19 pandemic

73%

Success rate in ransomware attempts

51%

Organizations have encountered ransomware in their environment

"Ransomware is a problem that's continuing to get bigger"

-Verizon Data Breach Investigations Report, 2020

Cybereason



TECHNOLOGY NEWS MARCH 31, 2021 / 11:22 AM / UPDATED 12 DAYS AGO

Ransomware tops U.S. cyber priorities, Homeland secretary says

By Raphael Satter

2 MIN READ



FILE PHOTO: U.S. Department of Homeland Security Secretary Alejandro Mayorkas speaks during a press briefing at the White House in Washington, U.S., March 1, 2021. REUTERS/Kevin Lamarque/File Photo

[source](#)



WHAT CHANGED?

Decline of "Spray and Pray":

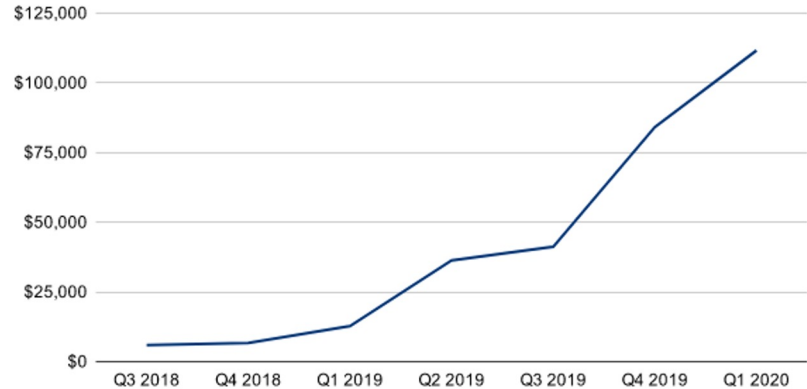
- Up until 2016, most ransomware attacks indiscriminately targeted individuals and organizations alike.

Bigger Risk, Bigger Payout:

- Since 2016, targeted attacks against organizations have increased dramatically.
- Average ransom rose from \$115k in 2019 to \$312k in 2020

Average Ransom Payment by Quarter

Amounts are in USD



FROM RANSOM TO BLACKMAIL TO EXTORTION

Concerning Trend:
**Shifting to
BLACKMAIL**

HOW CYBERCRIMINALS NOW FORCE VICTIMS TO PAY?

- Controlling the network can be used to steal data
- Data exfiltration at scale & stealth
- Don't want to pay? All your data will be sold to the highest bidder
- Exploiting the fear of legal ramifications (GDPR, HIPAA, PCI DDS, GLBA)

Ransomware in the News



National Cyber Awareness System > Alerts
> Ransomware Activity Targeting the Healthcare and Public Health Sector

Alert (AA20-302A)

Ransomware Activity

Original release

Cybersecurity

Colonial Pipeline Paid Hackers Nearly \$5 Million in Ransom

By William Turton, Michael Riley, and Jennifer Jacobs
May 13, 2021, 10:15 AM EDT Updated on May 13, 2021, 7:01 PM EDT

UKD Universitätsklinikum
Düsseldorf



DarkTracer : DarkWeb Criminal Intelligence
The number of victim organizations has exceeded...

CISA LAUNCHES CAMPAIGN TO REDUCE THE RISK OF RANSOMWARE

Original release date: January 21, 2021 | Last revised: February 16, 2021

WASHINGTON – The Cybersecurity and Infrastructure Security Agency (CISA) announced the Reduce the Risk of Ransomware Campaign today, a focused, coordinated and sustained effort to encourage public and private sector organizations to implement best practices, tools and resources that can help them mitigate this cybersecurity risk and threat.



TO DOUBLE (TRIPLE AND NOW *QUADRUPLE*) EXTORTION

Let's start

10.08.2020

We are a new product on the market, but that does not mean that we have no experience and we came from nowhere. We received millions of dollars profit by partnering with other well-known cryptolockers. We created **DarkSide** because we didn't find the perfect product for us. Now we have it.

Based on our principles, we will not attack the following targets:

- Medicine (only: hospitals, any palliative care organization, nursing homes, companies that develop and participate (to a large extent) in the distribution of the COVID-19 vaccine).
- Funeral services (Morgues, crematoria, funeral homes).
- Education (schools, universities).
- Non-profit organizations.
- Government sector.

We only attack companies that can pay the requested amount, we do not want to kill your business. Before any attack, we carefully analyze your accountancy and determine how much you can pay based on your net income. You can ask all your questions in the chat before paying and our support will answer them.

We provide the following guarantees for our targets:

- We guarantee decryption of one test file.
- We guarantee to provide decryptors after payment, as well as support in case of problems.
- We guarantee deletion of all uploaded data from TOR CDNs after payment.

If you refuse to pay:

- We will publish all your data and store it on our TOR CDNs for at least 6 months.
- We will send notification of your leak to the media and your partners and customers.
- We will **NEVER** provide you decryptors.

We take our reputation very seriously, so if paid, **all guarantees will be fulfilled**. If you don't want to pay, you will add to the list of published companies on our blog and become an example for others.



Sympathy for the DarkSide

(It's not exactly an apology)

DarkSide Leaks



About the latest news.

10.05.2021

We are apolitical, we do not participate in geopolitics, **do not need** to tie us with a defined government and look for other our motives.

Our goal is to make money, and not creating problems for society.

From today we introduce moderation and check each company that our partners want to encrypt to avoid social consequences in the future.

“Declaration of Henry Every to English ship commanders”

To all English Commanders lett this Satisfye that I was Riding here att this Instant in ye Ship fancy man of Warr formerly the Charles of ye Spanish Expedition who departed from Croniae ye 7th of May. 94: Being and am now in A Ship of 46 guns 150 Men & bound to Seek our fortunes **I have Never as Yett Wronged any English or Dutch nor never Intend while I am Commander.**

Wherefore as I Commonly Speake wth all Ships I Desire who ever Comes to ye perusal of this to take this Signall that if you or aney whome you may informe are desirous to know wt wee are att a Distance then make your Antient Vp in a Ball or Bundle and hoyst him att ye Mizon Peek ye Mizon Being furled I shall answere wth ye same & Never Molest you: for my Men are hungry Stout and Resolute: & should they Exceed my Desire I cannott help my selfe.

as Yett

An Englishman's friend,

At Johanna February 28th, 1694/5

Henry Every

Here is 160 od french Armed men now att Mohilla who waits for Opportunity of getting aney ship, take Care of your Selves.



Self-Styled Privateers?



briankrebs 
@briankrebs



Pro tip for the "but how do we protect ourselves?" folks. DarkSide ransomware, like many other strains, will not install on systems where certain Cyrillic keyboard and other scripts are already installed. So, install the Russian keyboard. You don't have to use it.

1:01 PM · May 11, 2021 · Twitter Web App

Benjamin Hornigold (1680-1719)

“Despite his apparent maritime supremacy, Hornigold remained careful not to attack British-flagged ships, apparently to maintain the legal defence that he was a privateer operating against England's enemies in the War of the Spanish Succession. This scrupulous approach was not to the liking of his lieutenants, and in the summer of 1716 a vote was taken among the combined crews to attack any vessel they chose.”



The Nation State Connection

State sponsored? Or State ignored?

The Russia Connection

Threshold of attack severity

Recent arrests - REvil

Money laundering in Moscow Financial District

Ransomware killswitch for Cyrillic keyboard



July 10, 2021
12:36 AM PDT
Last Updated 7 months ago

Technology

Biden presses Putin to act on ransomware attacks, hints at retaliation

By Steve Holland and Andrea Shalat

4 minute read



Ransomware as Camouflage

THN The Hacker News 
@TheHackersNews

Iranian APT hackers "Moses Staff" deploying a new Trojan—StrifeWater—in their #ransomware operations, which collects system files, executes commands, captures screenshots, creates persistence, and downloads updates and add-on modules.

Details: thehackernews.com/2022/02/hacker...

#infosec



thehackernews.com
Hacker Group 'Moses Staff' Using New StrifeWater RAT in Ransomware Attacks
Iranian APT hackers "Moses Staff" deploy a new Trojan called "StrifeWater" in the initial phase of their ransomware operations.

1:18 AM · Feb 2, 2022 · Twitter Web App

Ransomware by Partisan Groups

Belarusian activists launch ransomware attack in protest of dictatorship, Russian troop surge

The Belarusian Cyber-Partisans demanded the release of 50 political prisoners and the removal of all Russian troops from the country.



Written by **Jonathan Greig**,
Staff Writer

on January 24, 2022 | Topic: Ransomware

“Patriotic” Ransomware Cartels



WIRED 
@WIRED



A cache of 60,000 leaked chat messages and files from the notorious Conti ransomware group provides glimpses of how the criminal gang is well connected within Russia.




wired.com



Leaked Ransomware Docs Show Conti Helping Putin From the Shadows

Members of the hacker gang may act in Russia's interest, but their links to the FSB and Cozy Bear hackers appear ad hoc.

2:00 PM · Apr 2, 2022 · SocialFlow

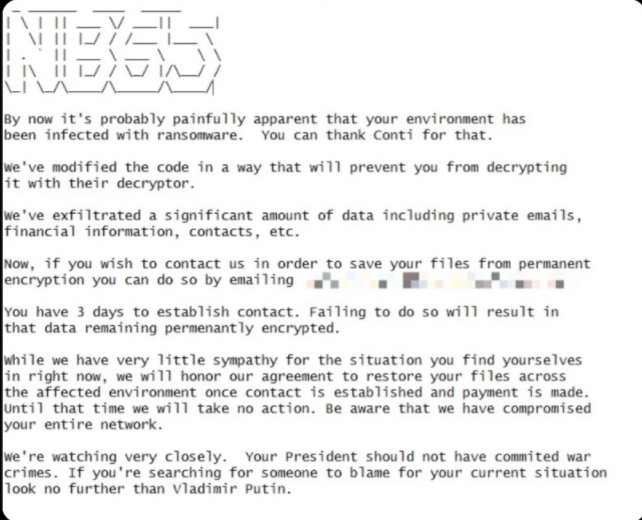
The Rise of Ransomware Activists

 **DarkFeed**
@ido_cohen2

 NB65 #Ransomware spotted in the wild 
No website only email address for ransom payments

"By now it's probably painfully apparent that your environment has been infected with ransomware. You can thank Conti for that"

#Conti ?



The screenshot shows a ransomware note with a logo at the top that reads "INTELS" in a stylized, blocky font. Below the logo, the text reads: "By now it's probably painfully apparent that your environment has been infected with ransomware. You can thank Conti for that." The next paragraph says: "We've modified the code in a way that will prevent you from decrypting it with their decryptor." The following paragraph states: "We've exfiltrated a significant amount of data including private emails, financial information, contacts, etc." The next paragraph says: "Now, if you wish to contact us in order to save your files from permanent encryption you can do so by emailing [redacted email address]". The following paragraph says: "You have 3 days to establish contact. Failing to do so will result in that data remaining permanently encrypted." The next paragraph says: "While we have very little sympathy for the situation you find yourselves in right now, we will honor our agreement to restore your files across the affected environment once contact is established and payment is made. Until that time we will take no action. Be aware that we have compromised your entire network." The final paragraph says: "We're watching very closely. Your President should not have committed war crimes. If you're searching for someone to blame for your current situation look no further than Vladimir Putin."

7:19 AM · Apr 11, 2022 · Twitter Web App

The Rise of Cyber Militias



Mykhailo Fedorov ✓

@FedorovMykhailo

🇺🇦 Ukraine government official



We are creating an IT army. We need digital talents. All operational tasks will be given here: t.me/itarmyofurraine. There will be tasks for everyone. We continue to fight on the cyber front. The first task is on the channel for cyber specialists.



t.me
itarmyofurraine
@lyosu

1:38 PM · Feb 26, 2022 · Twitter for iPhone

Attacks on the Strategic Sectors

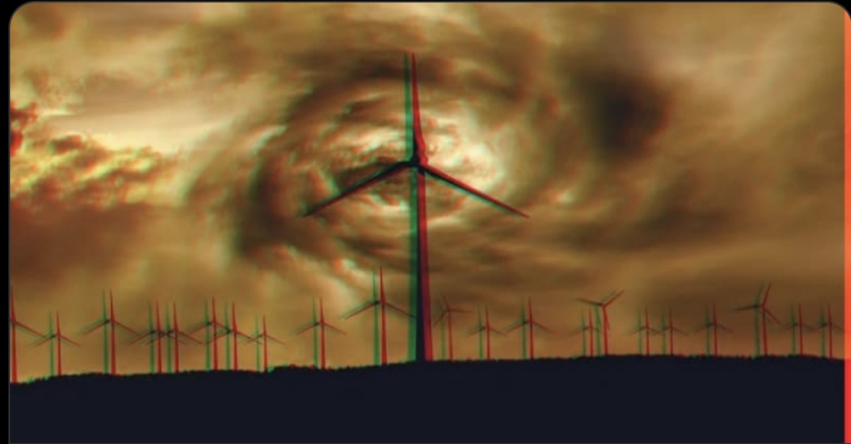


Hackread.com @HackRead · Apr 15

⚠️ The pro-Russian **#Conti ransomware** gang has claimed responsibility for the crippling cyberattack on **#Nordex**, a European giant that manufactures wind turbines.

Read: hackread.com/conti-ransomwa...

#Security #CyberAttack #Ransomware #Germany



hackread.com

Conti Ransomware Gang Hits German Wind Turbine Giant Nordex

Follow us on Twitter @HackRead - Facebook @ /HackRead


Costa Rica Crippled

“We are at war.”

- Costa Rican President Rodrigo Chavez

“FOR COSTA RICA”

<https://www.hacienda.go.cr/>
<https://www.mtss.go.cr>
<https://fodesaf.go.cr>

 We heartily congratulate Rodrigo Chavez on his victory! And we hope for further cooperation and friendship in the field of protecting the country from dangerous hackers, who, unlike us - professionals, do not keep their promises, I'm sure we can agree with you, in the chat we are open for private dialogue, for any of your questions, keep stability in your beautiful country, you have beautiful nature, educated young people, developed business, we are waiting for you in the chat

PUBLISHED 65%

4/23/2022


10530

READ MORE >>

Questions?