

# RIISING FROM THE ASHES

How 1 MSP Managed a Mass Scale Ransomware Attack

*Presented by*  
ROBERT CIOFFI  
PROGRESSIVE COMPUTING INC.

**JULY 2 2021 10:49AM-12:30PM EST**



# The first pelt of hailstones arrive...

Something bad just happened



Jim Cioffi <jc[REDACTED]@[REDACTED].com>

To  Robert Cioffi

 Reply

 Reply All

 Forward



Fri 7/2/2021 12:43 PM

 You replied to this message on 7/2/2021 1:56 PM.

**EXTERNAL SENDER** Use caution with links, attachments or requests for sensitive information.

Robert,

Several, if not all, [REDACTED] users have lost outlook on their desktop and lost their use of shoretel phones. Situation is urgent.

Get [Outlook for iOS](#)

Get [Outlook for iOS](#)

URGENT:

URGENT: [REDACTED] users have lost outlook on their desktop and lost their use of shoretel phones. Situation is urgent.

**LASCIATE OGNE SPERANZA VOI CH'INTRATE  
ABANDON ALL HOPE YE WHO ENTER HERE**



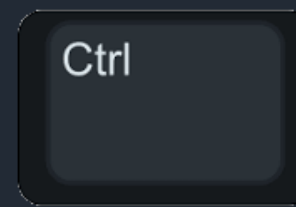
If you are going  
through hell  
keep going.

~ Winston Churchill





# WHERE IS THE



COMMITMENT

TEAM

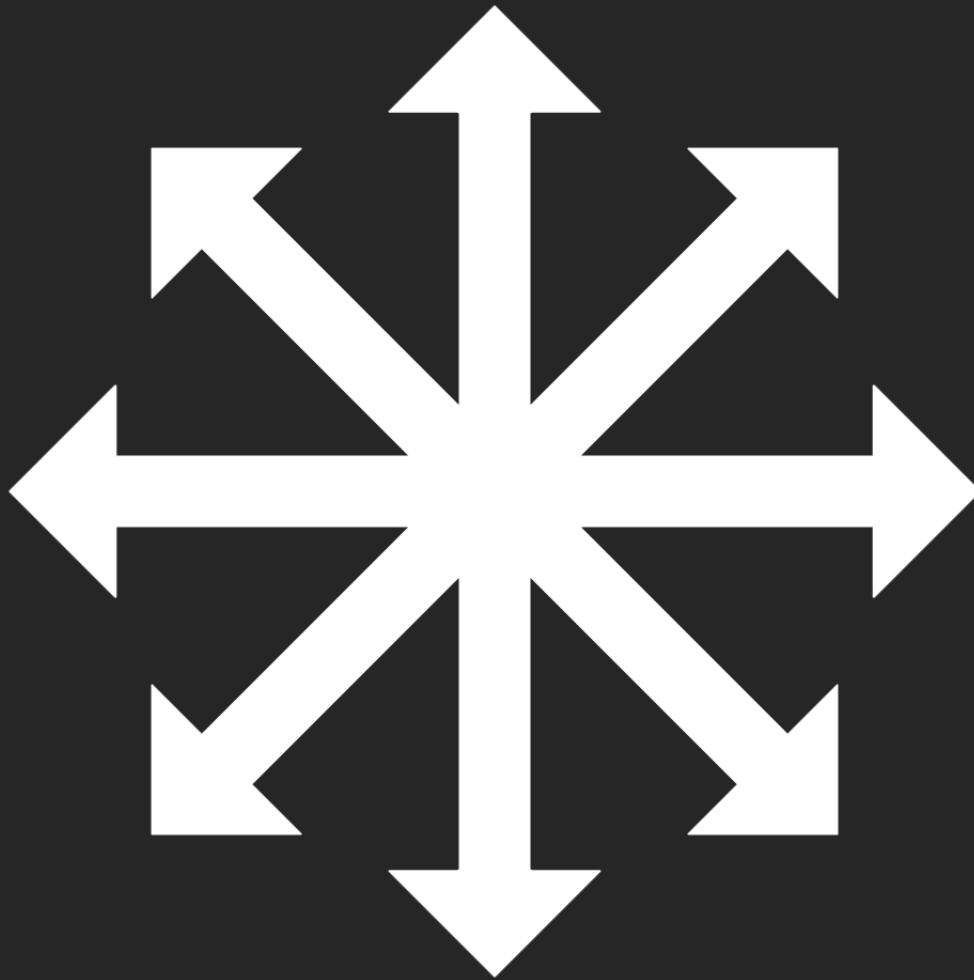
HUMBLE  
CONFIDENCE


RESPECT

Our **CORE VALUES** became a critical asset is helping us navigate a completely new & unknown situation.

**CULTURE** – of all things – was going to ultimately be a key factor in our survival.

**JULY 2 2021 / 1PM-12AM went like this...**





Then...  
we waited...  
*IM*PATIENTLY...  
for 48 HRS...  
Saturday (July 3)...  
Sunday (July 4)...  
... and finally...  
we had an RPO.





Jul 5, 2021 5:04 PM  
Kevin MacArthur

Robert and Ugo may get mad at me but I don't care.

SN has 2 bodies going to NY Tomorrow to help. One from FL and one from the cape. If anyone can get resources to NY in a day or so DO IT!!!

PCI is in a situation that we all would hate to be it. Step the F\*\* up and help out boys. Period!!!

Let Gooooo. PCI is weeks from recovery. Let's do what we need to do to make that's days. I will cover all expenses if needed. Help our boys out. Come one. Make it happen

If everyone can get 1-2 resources on a plane tomorrow we can tackle this crap as a team. Go go go!!!!

Kaseya today. Lab tech tomorrow. Don't let Karma bite you in the ass.

Hotels in Yonkers are awaiting your reservation. Make it happen!!!

Kevin



# ENCOUNTERS IN HELL



```
admin@myserver:~$ kill -s alldaemons
```

DATA EXFILTRATION

BACKUP FAILURE

TOOLSET COMPROMISE

SCALE OF ATTACK

TIMING OF ATTACK

NO IRP

DISREGARD PROCESS

POOR LEADERSHIP

NEGLIGENCE/FAULT

WEAK AGREEMENTS

LACKING INSURANCE

NO LEGAL ADVOCATE

LAWSUITS

NO COMMUNITY HELP

BAD VENDOR SUPPORT

COMPLIANCE VIOLATION

MONEY STOLEN

REVENUE LOSS

STAFF EXODUS

REPUTATION LOSS

EMOTIONAL STRESS

PHYSICAL IMPACT

PERSONAL RUIN

BUSINESS CLOSURE



# Angels & Saints

Axcient



CONNECTWISE™



ITNATION  
EVOLVE



PLUS 27 other subcontractors!



# IRL VILLAINS



YAROSLAV VASINSKYI



YEVGYENIY IGORYEVICH POLYANIN



## The DEMAND...

- From Kaseya: \$70 million
- From Each Customer: \$6 million
- For Each File Type: \$45,000



----- Welcome. Again. -----

[ - ] Whats HapPen? [ - ]

Your files are encrypted, and currently unavailable. You can check it: all files on your system has extension 6ym9ndu.  
By the way, everything is impossible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).

[ + ] What guarantees? [ + ]

Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we dod not do our work and liabilities - nobody will cooperate with us. Its not in our interests.  
To check the ability of returning files, You should go to our website. There you can decrypt on file for free. That is our guarantee.  
If you will not cooperate with our service - for us, Its does not matter. But you will lose your time and data, cause just we have the private key. In practice - time is much more valuable than money.

[ + ] How to get access on website? [ + ]

You have two ways:

- 1) [Recommended] Using a TOR browser!
  - a) Download and install TOR browser from this site: <https://torproject.org/>
  - b) Open our website: <http://-- REDACTED --.onion/-- REDACTED -->
- 2) If TOR blocked in your country, try to use VPN! But you can use our secondard website. For this:
  - a) Open your any browser (Chrome, Firefox, Opera, IE, Edge)
  - b) Open our secondary website: <http://decoder.re/-- REDACTED -->

Warning: secondary website can be blocked, thats why first variant much better and more available.

When you open our website, put the following data in the input form:  
Key:

-- REDACTED --

!!! DANGER !!!

DONT try to change files by yourself, DONT use any third party software for restoring your data or antivirus solutions - its may entail damge of the private key and, as result, The Loss all data.

!!! !!! !!!

ONE MORE TIME: Its in your interests to get your files back. From our side, we (the best specialists) make everything for restoring, but please should not interfere.

!!! !!! !!!



POWERPOST

# The Cybersecurity 202: The Kaseya attack is a ransomware

**Krebs on Security**  
In-depth security news and investigation

Subscribe

Markets  
DOW  
\$30,500

TechRepublic

Kaseya supply chain attack impacts more than 1,000 companies



by Lance Whitney in Security

## Kaseya Attack Suspect Arrested in Poland

Justice Department officials Monday said one suspected member of REvil, Ukrainian national Yaroslav Vasinskiy, 22, was arrested on Oct. 8 in Poland. The U.S. is now seeking his extradition.

for the criminal hacking  
businesses.

Blogs

Photo Galleries

Podcasts

Press Releases

Speeches

Videos

Ransom

Monday, November 8, 2021

Share

Justice Department  
Extortionists

The Justice Department ar

**Kaseya**

Last week cybercriminals deployed ransomware to 1,500 organizations, including many that provide IT security and technical support to other companies. The attackers expl

against two foreign nationals



# Is there Justice?



U.S. Department of Justice - VNS - Investigative Case 288R-DL-3155034 - Court Case 21-CR-00366



U.S. Department of Justice - VNS <fedemail@vns.usdoj.gov>  
To Robert Cioffi

☺ Reply Reply All → Forward

Fri 5/26/2023 11:55 AM

**EXTERNAL SENDER** Use caution with links, attachments or requests for sensitive information.

DO NOT REPLY TO THIS EMAIL.



May 26, 2023

Progressive Computing  
Mr. Robert Cioffi, C

Re: United States  
Case Number

Dear Mr. Cioffi, Co

The enclosed information and  
information and se  
investigation of the

The sentencing hearing  
TX 75242-1310 before

Court. If you plan on attending, you may want to verify the date and time by using the VNS Call Center or website. If you are a victim of the charged offense(s) and wish to speak at sentencing, please call our office well in advance of the scheduled hearing date.

The sentencing previously scheduled for defendant(s) Yaroslav Vasinskiy on June 20, 2023, 11:30 AM at US Courthouse, Courtroom 1632, 1100 Commerce St., Dallas, TX 75242-1310 has been cancelled. VNS will continue to provide you with updated case scheduling and event information.

A United States Probation Officer prepares a report for the Court and may contact you to discuss the impact the crime had on you financially, physically, and/or emotionally. If you are contacted, please make every effort to provide accurate and detailed information.

The sentencing hearing for defendant(s), Yaroslav Vasinskiy, has been set for **September 21, 2023, 11:30 AM** at US Courthouse, Courtroom 1632, 1100 Commerce St., Dallas, TX 75242-1310 before Judge Karen Scholer. **You are welcome to attend this proceeding**; however, unless you have received a subpoena, your attendance is not required by the Court. If you plan on attending, you may want to verify the date and time by using the VNS Call Center or website. If you are a victim of the charged offense(s) and wish to speak at sentencing, please call our office well in advance of the scheduled hearing date.

**The sentencing previously scheduled** for defendant(s) Yaroslav Vasinskiy **on June 20, 2023, 11:30 AM** at US Courthouse, Courtroom 1632, 1100 Commerce St., Dallas, TX 75242-1310 **has been cancelled**. VNS will continue to provide you with updated case scheduling and event information.

**Guilty**

# The Body Count...

80 Clients, 200 Sites, 4 Time Zones (PST-EST), 2500 endpoints.

We were 1 of ~60 Kaseya VSA customers attacked.

COOP Swedish Supermarket closes 500 stores for 5 days.

100 North Island Kindergartens in New Zealand.

Maryland towns of North Beach & Leonardtown via their MSP.

Hackers claimed they infected over 1 million systems.

# LESSONS LEARNED

# COMMUNICATION IS KEY

Not all communication  
is good communication

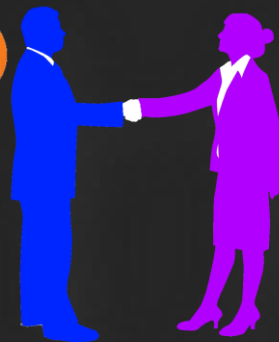


## WATCH YOUR C's

COUNSELED  
CONSIDERATE  
CONSISTENT  
CLEAR  
CONCISE

## AUDIENCES

CLIENTS  
INTERNAL  
VENDORS  
INS/LLEGAL/LAW  
FAMILY/FRIENDS



Don't Say:

**Breach**

Instead say:

**Incident or Attack**



# ROLES WILL CHANGE

## *LEFT OF BOOM*

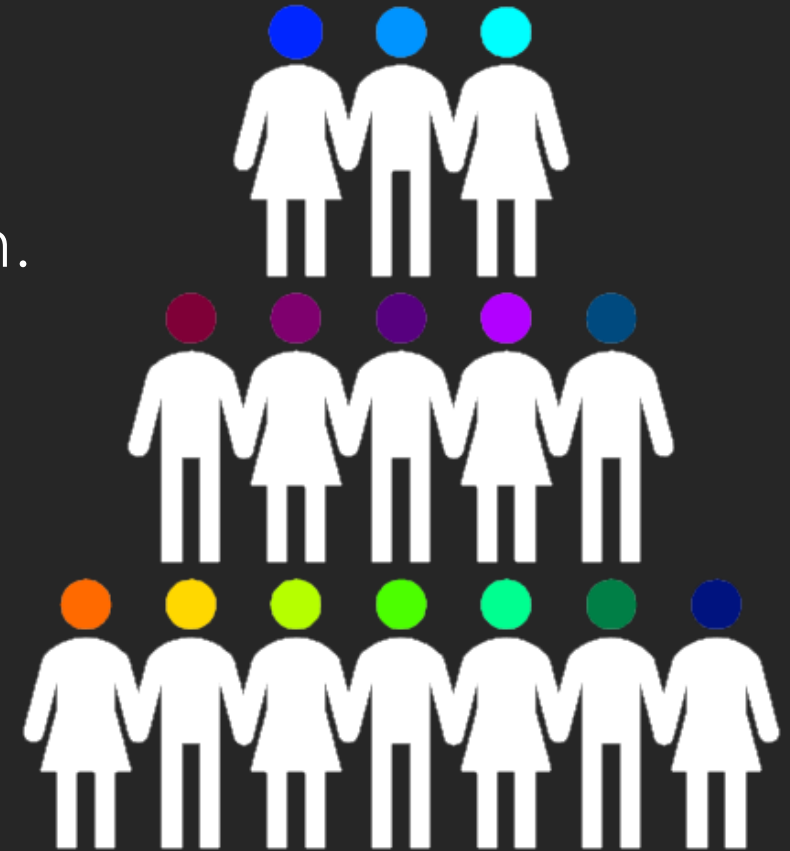


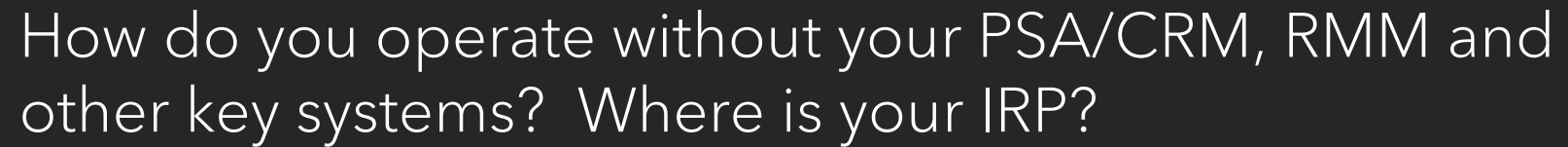
A high functioning company has well defined accountabilities for the entire team.



## *RIGHT OF BOOM*

Roles and responsibilities will change temporarily. You need to adapt quickly. Your team must be ready and willing to do different jobs.





Even if available, a mass scale recovery effort might require different tools, different strategy, and different behaviors.

[illegible]

Is it over  
yet?

Not  
quite...

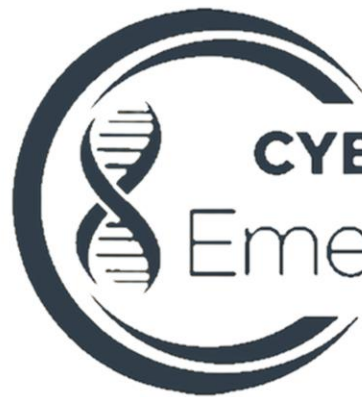


*Chapter 13*



# COMMUNITY

THE MISSING ELEMENT IN THE  
FIGHT AGAINST CYBER CRIMINALS



CompTIA

**CYBERSECURITY**

Emergency Response Team

[msp911.org](https://msp911.org)



ROBERT CIOFFI  
PROGRESSIVE COMPUTING INC.  
[robertc@progressivecomputing.com](mailto:robertc@progressivecomputing.com)  
<https://www.linkedin.com/in/rcioffi/>