NOV 2021 VOL. 1

NOTES FROM UG

HELLO,

WELCOME TO NOTES FROM UG. THIS IS VX-UNDERGROUND'S PUBLICATION IN WHICH, UNLIKE TRADITIONAL INTERVIEWS, WE ALLOW MEMBERS FROM OUR COMMUNITY TO ASK A THREAT ACTOR ANYTHING. THIS PUBLICATION WAS DESIGNED NOT TO GLORIFY OR ENDORSE THREAT ACTORS. THIS PUBLICATION IS ALSO NOT A PLACE WHERE THEY CAN PREACH THEIR PRODUCT. INSTEAD THIS SERIES ALLOWS US TO HUMANIZE THE INDIVIDUAL BEHIND THE COMPUTER. IT ALLOWS US TO UNDERSTAND WHO THESE PEOPLE ARE, WHY THEY DO THE THINGS THEY DO, AND ILLUSTRATE THAT THESE INDIVIDUALS ARE ALSO HUMAN. WE DO NOT EXPECT OUR READERS TO SYMPATHIZE WITH THEM, OR LIKE THEM AS HUMAN BEINGS. RATHER, WE HOPE THAT THROUGH THIS SERIES THAT WE CAN ACHIEVE SOME UNDERSTANDING ON THEIR PERSPECTIVE IN LIFE.

BECAUSE THIS SERIES ALLOWS ANYTHING TO BE ASKED THERE ARE MANY GOOD, AND INSIGHTFUL QUESTIONS, AND ALSO LOTS OF TROLL-ISH QUESTIONS. THREAT ACTORS WHO AGREE TO INTERVIEW DESIGNATE THE RIGHT TO DECLINE TO COMMENT AND, BECAUSE THIS IS NOT COURT, THEY ALSO MAY NOT TELL THE TRUTH.

WE ALSO ASK OUR READERS TO HAVE AN OPEN MIND, RELAX, AND WE HOPE YOU ENJOY THE SERIES.

-VX-UNDERGROUND TEAM

CONVERSE WITH KAJIT

VXUNDERGROUND

Do you live with paranoia stemming from getting caught and if so how does it affect your mental state in your day to day life?

I enjoy life - because I do what I love. I would do it even without money, it's just a little more fun to live with them, you know.

In the most general sense, is your way of life worth it?

I don't understand your question, are you asking if I'm satisfied with the results? - yes, I'm happy, I don't regret anything.

Can you give us free ransomware money?

Ye, I can. If you are a skillable kid.

How did you get recruited?

I was not recruited. I do the recruiting.

Favorite rappers?

NWA and Eminem. Fuck the police

If you could choose to have a white hat career of equivalent status to your criminal one, would you take it?

I was the white hat. But, those fat bastards from corporate looked at me like I was dirt.
It felt like I had to beg them for money. That is why I switched to a different "business" model.
Now my pentests will be paid what I believe they're worth.
Remember Max Butler? He wanted to help and look what happened to him.

What is the most common method of entry into a company?

I don't used most common methods. I don't know...
But, I think it is phishing.

The most important security hole is the gasket between the keyboard and the chair.

Would you consider to attack some companies more than others because of their bad practices or impact to the environment? Given that is profitable

Ye, we fucked some organizations that were engaged in the sale of Slaves. I am always willing to assist Interpol when it comes to the Slave trade.

What skills are required for a successful ransomware operation?

It is like a Red-teamer, but many more times harder. When we begin our pentests the white hats are getting off their AV/EDRs
When they begin making their silly YouTube videos -
We need to totally fuck the system and outplay the EDR and Protection systems.

Have you ever failed a ransomware operation and if so, did you learn anything from it?

Of course, everyone makes mistakes. We draw conclusions based on the results of any operation. We always sum up at the end.

How did you start hacking?

My Commodore 64 Games System broke down very often and I had to fix it. In the USSR it was very difficult, I had to master the debugger... in '89 we didn't even have documentation.
I had to disassemble the binaries into pieces. First exploits and malware were written, then the ransoms began.

> **THE FUTURE BELONGS TO ARM - 100%**
>
> -- KAJIT

HOW MUCH HAVE YOU MADE?

$33,000,000

NOTE: *KAJIT STATED 33KK

WHAT WOULD YOU DO IF ALL CRYPTOCURRENCY WAS BANNED IN THE US?

I WILL RAISE THE REDEMPTION PRICE. BECAUSE THE PAYER WILL HAVE TO HIDE THE PURCHASE OF THE CRYPTOCURRENCY. I WILL ALWAYS BE PAID. EVERYONE SINS.

HOW LONG DOES AN OPERATION USUALLY TAKE?

SOME 3 HOURS, SOME 3 MONTHS, SOME AS LONG AS A YEAR. (SUCH AS A SUPPLY CHAIN ATTACK)

DO YOU WANT A BIG TITTY GIRLFRIEND?

YE, I LIKE BIG TITTIES SO MUCH

WHAT THE MOST EFFECTIVE WAY YOU CLEAN YOUR MONEY?

JUST USE MONERO, BRO.

What is the biggest threat to your operations?

I don't see any threats to myself. If you are interested in reading on how our operations are disrupted. Read your Threat Intel reports.

Do you do anything, besides ransomware, for money?

Espionage - selling others information too. This is rare though.

What have you used the money you got from ransoms towards?

Buying flowers and diamonds for girls

Do Russian criminals really all go to the Black Sea for holidays?

I don't know.

What is the funniest thing you've come across online about you?

The story of how we extorted an Israeli ISP in the 90s. So funny

Did you ransom an Israeli ISP in the 90s?

Ye, but the journalists exaggerated it.

Is there anything you'd like to tell people?

You know, I have a lot of friends in America and they thank me for what I do. As a result of my actions your society will learn about its weaknesses
Imagine a situation, a war begins with China. China would 100% attack cause a second Colonial pipeline incident
Many of my people are Chinese - they are good specialists

How prevalent are custom toolings these days? It seems no one bothers write their own tools anymore

No, that's not true. those who really know how to work have been rewriting cobalt for themselves for a long time.
In its pure form, it cannot be used. To think that ransom actors work like this is a big misconception.

With the recent arrests of gangs from NetWalker, Cl0p, Egregor, has this changed the attitude of ransomware operators outside of Russia? Are they more cautious? Is the demand now much higher than supply?"

I can't say about my colleagues. such things are not usually discussed. I feel great.

Do you like femboys?

No

How many supercars do you own?

None. I like fighter jets better.

Have you attended any formal University?

"Basic Programming" cartridge for the Atari 2600 - that's my teacher.

Do you celebrate Christmas? If so, what do you want from Santa?

Oh so cute.
0day for LPE

Any siblings?

My brother in arms only.

There are few samples and limited resources for ransomware - is there something special resource we are missing?

I wanted to make money, and decided to pwn some companies. It was easy. Find your first hole from a port scan - begin doing something bad. You can do anything you want. You just need to work hard. Never give up, buddy.

HOW LONG HAVE YOU BEEN RUNNING RANSOMWARE CAMPAIGNS?

Ask Threat Intel.

WHAT INDUSTRY IS MOST LIKELY TO PAY RANSOMS, FROM YOUR EXPERIENCE?

Hosters - 99%
Datacenters and data-mines too

DOTA 2 OR WC3?

wc3 - 100% It is the best.
The new shit remastered needs to die. Lets go back to 2004.

WHAT DO YOU THINK OF MY MERCEDES? WANNA DRAG RACE THROUGH KUTUZOVSKY PROSPEKT? YOUR LAMBORGHINI VS MY AMG.

My Porsche Taycan(2sec -> 100km\h) can fuck any car with a gasoline engine. So relax, boy.

FAVORITE PIZZA TOPPINGS?!?

Pepperoni. It is the best.

HOW CAN I BECOME LIKE YOU, KAJIT?

Just work 16hrs a day, buddy!

DO YOU HAVE ANY PETS? IF SO, HOW MANY?

I have 2 cats. I like them, but I want to buy some Mantis Shrimp. They look like Pokemon.

FAVORITE SPORT?

Shooting. I love my G36 so much. I also like revolvers.

DREAM VACATION?

I don't know, anywhere with lots of forests.
I like walking through them so much.

DO YOU LIKE FREEBSD?

Ye, but I prefer to build my own Linux core. I don't trust anyone anymore.

WHAT BROWSER DO YOU USE?

Curl

WHAT IS YOUR FIRST NAME, LAST NAME, DATE OF BIRTH, AND ADDRESS?

Vladimir Vladimirovich Putin - Moscow city

DO YOU LIKE APPLE PRODUCTS?

No, but I like the new M1 processors.

HAVE YOU EVER TRASHED YOUR LAB WHILE TESTING RANSOMWARE?

My lab is United States businesses. I don't need a lab.

Are you targets intentional? Or is it random?

My targets are those with sins. 100%. I don't need to use a locker. It is always planned. The located of the business does not matter to me.

Will you join our Discord?

No

Have you seen any new and cool persistence methods used in ransomware?

I've stopped using ransomware so I cannot comment on current methods. Now for big targets, we use ring0.

Do you use OS specific tools?

Yes. All tools are OS specific and, in some cases, regionally specific.

Does it bother you that you make a lot of money but cant spend it?

Hahahaha. Don't worry, bro. We can spend our money.

Does the Russian government know who you are?

I don't know. Maybe?

Does it bother you that you hurt people?

No

What was the easiest hack you've done against a big company?

One time our TrickBot instance sent us credentials from Pulse VPN. Pulse VPN was running on the DC. Hahahahaha. The DC was our access point. Within 20 seconds we ransomed 5,000 PCs. No one stopped us - it happened in the middle of the night.

If you weren't into computers, what would you do?

I would probably be a Neurobiologist.

Do you like Linus Tech Tips on YouTube?

I don't know. I don't really watch YouTube. I prefer to read.

What enterprise security products do you run into the most?

Sophos, SentinelOne, and FireEye. Tell them they owe me some money hahahahaha
Without us they wouldn't be needed. Hahahahaha

Did you do well in High School?

Yes, but I had hard times with non-scientific classes. I did not do well in language lessons I spent more time focusing on our scientific topics. I knew what I wanted to learn. I did not care about philosophy or history.

When you started hacking - did you have a nice computer? Or was it a piece of junk?

My first 'good' PC was in, probably, 2005. It was an AMD Athlon 64 4000+.
Damn, it was so cool that year.

Which security product make your life harder when trying to deploy your tools?

SentinelOne and FireEye.
I hate those fuckers. Now you guys owe me one.

Do you ever outsource as legitimate work?

Ye, it is common practice in IT.

Do you have your OB security clearance?

I don't know what this means.

HAVE YOU EVER EXPERIENCED BURN OUT? WHAT DO YOU DO TO STAY MENTALLY HEALTHY?

I'm happy - I don't need anything, I'm healthy, I have a hobby. It's a rare person who has so much.

DO YOU LIKE "DARK ART?"

Ye, I like it, buddy.

FAVORITE VIDEO GAME?

Skyrim, obviously.

IF TWO MEN ARE HAVING SEX, AND THERE BALLS DONT TOUCH, IS IT STILL CONSIDERED GAY?

What the fuck? Hahaha. I do not go to gay clubs - I hate gay people. Bro, Lesbians are okay. But gay men? No.

HOW WILL YOU EXPLAIN YOUR ACTIONS TO YOUR CHILDREN?

Easy, bro. I had a goal and the price didn't matter.

DO YOU LIKE KALI OS?

No.

WHATS YOUR COMPUTER SPECS?

Right now I've got 256GB of RAM, 64core processor, and 10TB of SSD disk space.

THOUGHTS ON THE GAME HACKING/"PAYTOCHEAT" SCENE?

I think it is a good business. It is interesting.
I made some once - used a lot of IDA, I enjoyed the puzzle.

IS YOUR DICK BIGGER THAN 6 INCHES?

/me runs for ruler

IF I PAID FOR YOUR FLIGHT TO THE UNITED STATES, WOULD YOU COME?

Hahahaha. NO. Why are Feds so stupid? Hahahaha

WHAT IS YOUR LONG TERM GOAL? WILL YOU RETIRE SOON?

I'd like to finance research on genetics, neurobiology, or physics.

Ever thought about after making a lot of money, what will you do with the money when you're dead?

I will not die, I will live forever. Or they will kill me. My death will not be from old age. I do not worry about this at all.

Have you ever read Incident Reports from your attacks (private or public)?

Ye, I do it everyday.

Who is your next target?

USA Gov departments.

If you have kids, friends or family members who want to get into this stuff. Would you consider supporting them or would you try to keep them out of this?

I would not support them.

How annoying are malware analysts to what you do?

They are not annoying.

How would you feel if your family was hit by ransomware and lost important data that they could not recover?

I do not have a family. It cannot be imagined how I would feel Just do god damn backups.

Have they banned anyone from a prominent ransomware group?

No

Governments has seized crypto currency in the past, how do you store money in the event that you get raided?

Governments have seized cryptocurrency in the past. They will have to try to seize mine))

Who do they feel is the “best” group?

REvil. They will be back - but under a different name.

What’s the best language for ransomware?

MASM

Do you train people in your craft?

Ye, of course we do.

Do you write code from scratch? Or do you use different peoples frameworks?

I do both.

What physical assets do you invest in? How do you secure those assets in the event of a raid?

(No comment)

A lot of articles call ransomware "crimeware" and I've seen mentions of "organized crime families" is this crime mob stuff bullshit?

Bro, most high level Red-teamers (I dont like the word "hacker", Dennis MacAlistair Ritchie - was a hacker, we are not) ... Red-teamers rely less on RaaS now. We just need their sensitive data.

When you are done with your part of the ransomware operation how do you feel?

I feel like I need a new target and I need more exploits. Nowadays good exploits are harder to get

What is the weirdest environment you've seen?

Acti-lab honeypots