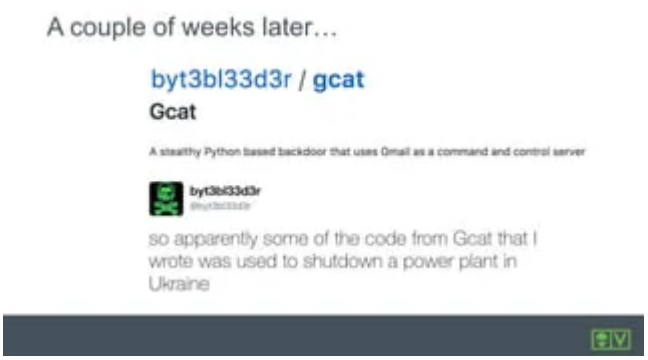
Open Source Malware - Sharing is caring?

Archived: 2026-04-05 22:31:53 UTC



An (extreme) worst case

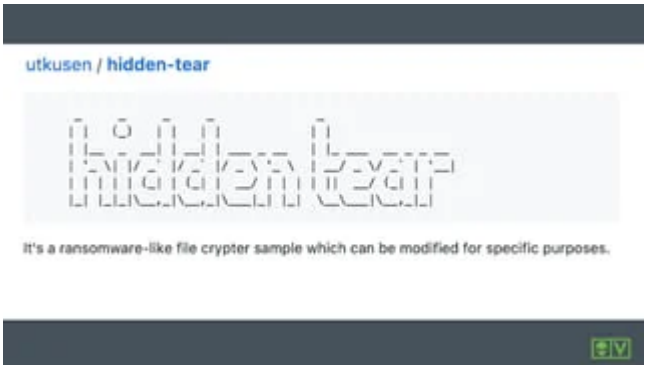
December 2016

Via ESET

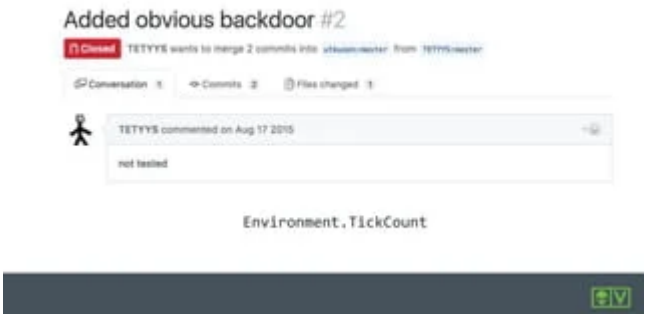
Ukraine investigates suspected cyber attack on Kiev power grid


jgamblin / Mirai-Source-Code
[FREE] World's Largest Net:Mirai Botnet, Client, Echo Loader, CNC source code release
Anna-senpai
Preface


Nearly One In Twenty Deutsche Telekom users Targeted By Mirai Botnet Clone
TalkTalk and Post Office routers hit by cyber-attack


utkusen / hidden-tear
It's a ransomware-like file crypter sample which can be modified for specific purposes.


Files have been encrypted by Hidden tear
Send me some bitcoin or hmmm.....or COOOOOKIIIIIIIIIII
And I also hate night clubs, desserts, being drunk.


Added obvious backdoor #2
Closed
TETYYS wants to merge 2 commits into
from
Conversation 1
Commits 2
Files changed 1
TETYYS commented on Aug 17 2015
not tested
Environment.TickCount


!!!!!! ATENÇÃO !!!!!!
TODOS OS SEUS ARQUIVOS FORAM TRANCADOS !!!
PARA QUE HAJA O DESBLOQUEIO DO MESMO, ACESS
ARQUIVO "MENSAGEM" CRIADO NA SUA ÁREA DE TRA
APÓS ACESSAR O ARQUIVO ENCONTRARÁ INTRUÇÕES
A LIBERAÇÃO DE TODOS OS SEUS ARQUIVOS !
CASO NÃO SIGA AS ETAPAS, TODO O SEU COMPUTAD
SERÁ DELETADO !!!
SEM SEGUIR AS INSTRUÇÕES DA MENSAGEM É IMPOS
RECUPERAÇÃO DOS ARQUIVOS !!!!


Utku Sen @utku1337 14 Jan 16
first of all I'm not "Turkish security group Otko Sen" blog.trendmi-
cro.com/trendlabs-secu... pic.twitter.com/fIXmAt05wAz
Utku Sen
@utku1337
Takip et
Anyway I believe I can decrypt it if @TrendMicro team send me
the malware
14:40 - 14 Jan 2016
2


Decrypting HiddenTear


utkusen / eda2
It's a ransomware-like file crypter sample which can be modified for specific purposes. It's more extended version of hidden tear.


Buy Far Cry Primal Standard Edition
Add to Cart


3DM CRACK
FARCRY
PRIMAL
FAR CRY PRIMAL 3DM CRACK | New 3DM CRACK Working 100 % | September 2016


Looks like you've got a big problem.
Look at READ_IT.txt for the solution.

You'll never be able to find me. Police will never be able to find me.

I've been doing this for five years now and haven't been caught yet.

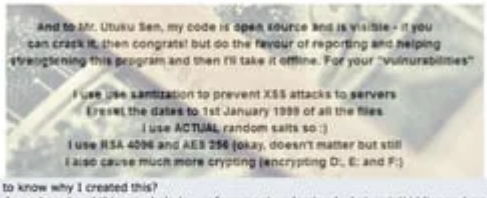
Best Buy will have no ability to undo the encryption. Hell, even the NSA probably couldn't undo it.

It's an eda2 variant. I retrieved the private keys from c&c server by using my backdoor. (It's still up 23.227.199.175)

Effected pc names (total=656) : http://ulkusen.com/pc.txt

Keys: http://ulkusen.com/keys.zip

empinel / **Win32.Stolich**



If anybody wants to know why I created this?
Simple... because I was bored and this may help law enforcement understand what scriptkiddies and maybe some ransomwares work like

I've found the eda2 backdoor (self-Malware)
submitted 1 year ago by Kiaat
[removed]

rudzen / Win32.Stolich

[redacted] is a 13 year old programmer and freelance altcoin developer from India.

Flames: If you think this is crap, you're probably right. Sue me

Yesterday…

Teen boy arrested on suspicion of creating ransomware virus

YOKOHAMA -- A 14-year-old boy was arrested on June 5 on suspicion of creating a ransomware virus, police said. "I did it because I wanted to increase my name recognition," he was quoted as telling police. He uploaded a comment to a social media site, saying, "I made ransomware. Please feel free to use it." There is a possibility that the

Magic Ransomware – EDA2 variant

```
All your files is encrypted with strong
encryption.
To unlock your files you must pay 1 to
address bitcoin:
1LXFUhLtEnJYTo2YyMhdUCBaHcgc6LaLfR
```

!!! Your php script has an error or account was terminated for terms infringement. Contact us if you need more details about this problem.

jeanclaudevandan, on 25 Jan 2016 - 10:58 PM, said:

This is just aexpriment we want to shutdown all opensource ransomwares if ufkusen take down hiddentear also and take responsibilty and send us 3 btc.we will send here all magic keys.

this offer only valid for 1 hour.

"I'm sorry, I failed this time."

This project is abandoned. If you are a researcher and want the code, contact me with your university or company e-mail http://ufkusen.com/en/contact.html

This project is abandoned. If you are a researcher and want the code, contact me with your university or company e-mail http://ufkusen.com/en/contact.html

Once your code is out there, it's out there

goliate / **hidden-tear**

etherume / **hidden-tear-1**
forked from ufkusen/hidden-tear

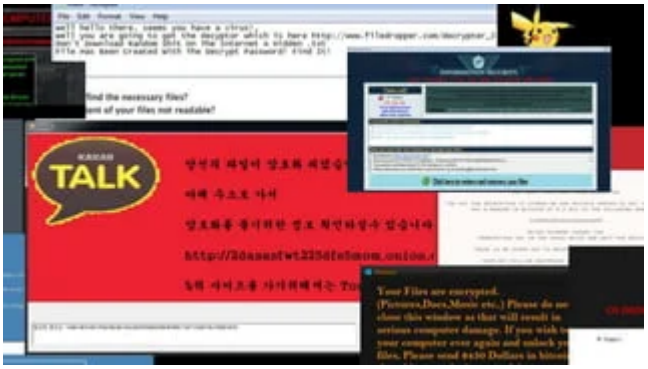
RamadhanAmizudin / **hidden-tear**
forked from goliate/hidden-tear

bitbeans / **ransodium**
like hidden-tear with libsodium

redpois0n / **native-tear**
Clone of hidden tear written in C++

MarcAngio / **Hidden-tear-2.0**
Hidden tear 2.0 with more extension and now it can crypt directory like Documents, Download, Pictures etc.

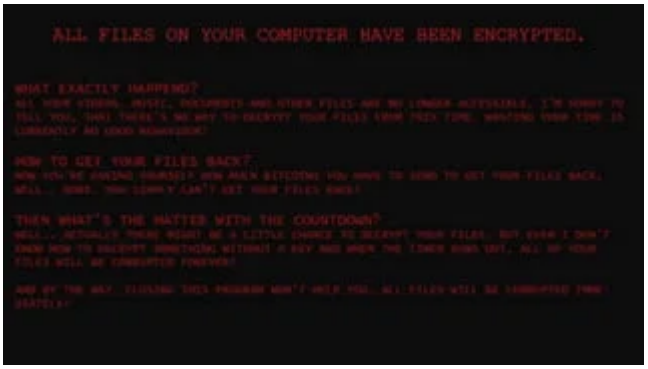

Для расшифровки вы
2
To decrypt you
BITCOIN
WARNING!
Your Files are encrypted.


TALK
Your Files are encrypted.


FSOCIET


1-844-816-232
FSOCIET


Hi,this is not your lucky day because this is not a joke, all your files has been encrypted with
If you want to retrieve all of your files I recommend you follow my simple instructions because
Send me
) to this address:
If you do not know what bitcoins are or you do not know how to buy them, I suggest you visit the official site
https://bitcoin.org/en
https://bitcoin.org/en/exchanges
After making the payment please contact me resurrection777@protonmail.com here you will receive the decryption key for your files.
You have
to make payment upon expiration of this expiration you will die forever all your files and your pc will be formatted.
I suggest you not to underestimate this message and to follow my instructions carefully

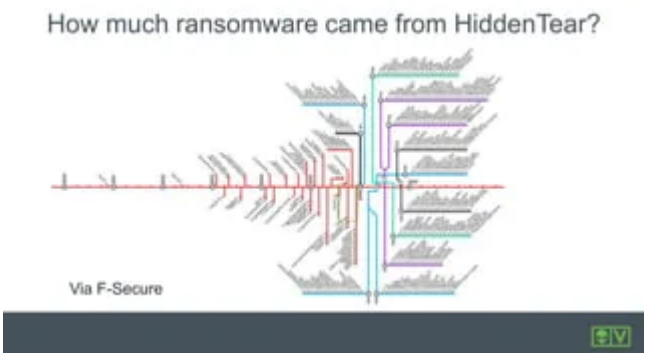

ALL FILES ON YOUR COMPUTER HAVE BEEN ENCRYPTED.
WHAT EXACTLY HAPPENED?
HOW TO GET YOUR FILES BACK?
THEN WHAT'S THE MATTER WITH THE COUNTDOWN?

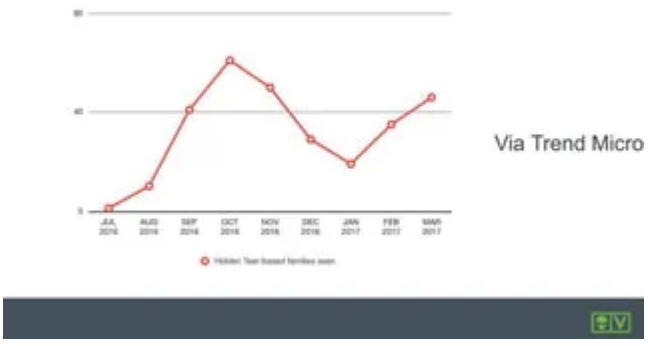

Your Files has been Encrypted!
3 DAYS
5 DAYS
BITCOIN
CHECK PAYMENT


WARNING!
What the HELL is it?
How can I recover my fil


Hello
Your computer has been infected by
the kindest Ransomware ever.
We will not take your money or
anything else from you, we just want
you to be more aware of ransomwares
about how it works. Now watch this
video while we are doing everything
a ransomware does.
If you want to be more aware go to


Dashboard
1
0
0
12845
Files encrypted


How much ransomware came from HiddenTear?
Via F-Secure


JUL 2016
AUG 2016
SEP 2016
OCT 2016
NOV 2016
DEC 2016
JAN 2017
FEB 2017
MAR 2017
Via Trend Micro

"hidden tear may be used only for educational purposes"

Open Source license?

Wassenaar?

WannaCry

RiskSense-Ops / **MS17-010**

MS17-010

"It appears that the ransomware took advantage of the published Python source … SMB structures found in the ransomware are identical to the published ones.

… most likely without even understanding how the EternalBlue exploit actually works"

Via BAE

rickey-g / fancybear

]HackedTeam[

Hacked Team

Quartermasters

Via PwC

Via ShadowServer

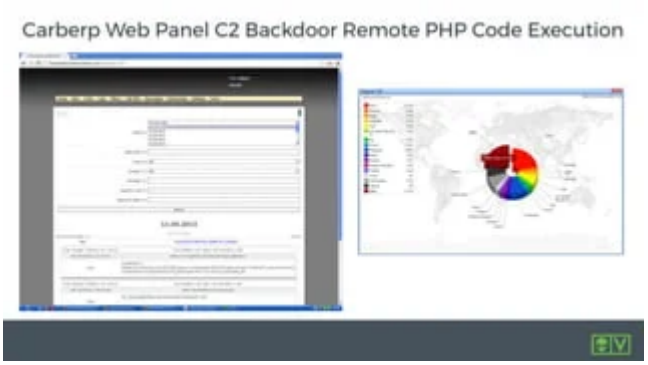
hzeroo / Carberp

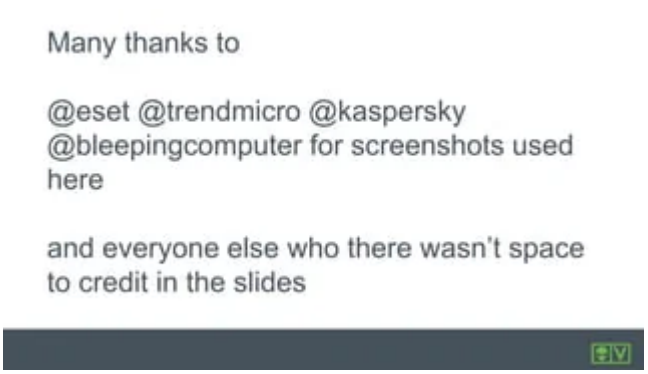
Sofacy Recycles Carberp and Metasploit Code

Also of interest is the CIA's borrowing of the Carberp, a powerful piece of bank-fraud malware that once fetched as much as $40,000 in underground forums. Once the Carberp source code was leaked in 2013, security experts warned it was akin to "handing a bazooka to a child."

All components were carefully analysed for hidden functionality and vulnerabilities

Is there an upside?





More Related Content

PDF

How to protect your business from Wannacry Ransomware

PPTX

Malware’s Most Wanted: NightHunter. A Massive Campaign to Steal Credentials R...

PDF

Wannacry | Technical Insight and Lessons Learned

PPTX

Blackhat USA 2014 - The New Scourge of Ransomware

PDF

Ransomware: Wannacry

PPT

Wannacry

PPTX

Shamoon attacks - Destructive malware targeting Middle East organizations

PPTX

Dragonfly: Western energy sector targeted by sophisticated attack group

What's hot

PPT

Protecting Your organization from WannaCry Ransomware

PPT

Wannacry-A Ransomware Attack

PPTX

ITPG Secure on WannaCry

PPTX

Ransomware 2017: New threats emerge

PDF

Hunting Layered Malware by Raul Alvarez

PPTX

Dissecting Cryptowall

PPTX

Threat landscape update: June to September 2017

PPTX

MMW April 2016 Ransomware Resurgence

PPTX

WannaCry Ransomware

PPTX

Wannacry

PDF

CSF18 - Guarding Against the Unknown - Rafael Narezzi

More from Christopher Doman

PDF

Minimizing Permissions for Cloud Forensics_ A Practical Guide for Tightening ...

PDF

Cloudgrep - Blackhat Aresenal - cloudgrep searches cloud storage

PDF

Cloud Detection & Response - GCP - Google Cloud

PDF

Cloud Detection & Response - Azure - Details

PDF

Cloud Detection & Response - AWS - Details

PDF

Cloud Detection & Response - Vendors.pdf

PDF

Cloud Detection & Response - Solutions -

PDF

Cloud Detection & Response Tools - Cloud Detection and Response (CDR) tools a...

PDF

Cloud Detection & Response - Definitions.pdf

PDF

Five Reasons Why You Need Cloud Investigation & Response Automation

PDF

Azure Incident Response Cheat Sheet.pdf

PDF

AWS Incident Response Cheat Sheet.pdf

PDF

A New Perspective on Resource-Level Cloud Forensics

PDF

Cloud Forensics Tools

PDF

Cloud Forensics and Incident Response Training.pdf

PDF

AWS Guard Duty Forensics & Incident Response.pdf

PDF

EKS Forensics & Incident Response.pdf

PDF

AWS IAM Forensics & Incident Response

PDF

AWS Forensics & Incident Response

PDF

Lambda Forensics & Incident Response.pdf

Open Source Malware - Sharing is caring?

- 1.
- 3.
- 4.
- 5.
- 6.
- 13.
- 16.
- 21.

You'll never beable to find me. Police will never be able to find me. I've been doing this for five years now and haven't been caught yet. Best Buy will have no ability to undo the encryption. Hell, even the NSA probably couldn't undo it.

- 28.
- 29.

Magic Ransomware –EDA2 variant All your files is encrypted with strong encryption. To unlock your files you must pay 1 to address bitcoin: 1LXFUhLtEnJYTo2YyMhdUCBaHcgc6LaLfR

- 31.
- 32.
- 36.
- 37.
- 43.
- 44.
- 45.

“hidden tear maybe used only for educational purposes” Open Source license? Wassenaar?

- 47.
- 48.
- 49.

“It appears thatthe ransomware took advantage of the published Python source … SMB structures found in the ransomware are identical to the published ones. … most likely without even understanding how the EternalBlue exploit actually works” Via BAE WannaCry

- 52.
- 54.

All components werecarefully analysed for hidden functionality and vulnerabilities

- 55.
- 58.

Many thanks to @eset@trendmicro @kaspersky @bleepingcomputer for screenshots used here and everyone else who there wasn’t space to credit in the slides

- 59.

Editor's Notes

- #2 - 1 minute Hey thanks for coming to the talk My name is Chris Doman, I’m work on Alienvaults threat intel platform called OTX You might also know me from another project called threatcrowd. I won’t bother with an introduction, but I’ll just say that I started in the industry thanks to the cyber security challenge who have a booth here today The talk today is on open source malware – I thought it’d fit nicely with

Bsides topic of sharing is caring Obviously like all software open source has been abused for a long time – but there seems to be growth in a couple of areas So to illustrate these threats – I'm going to tell a couple of stories today ___ ___ Deleted text: They gradually improved these open source programs to make them more subtle however, and these days they use their own almost entirely custom toolset Though twenty years on there are still some shadows of that 1990s phrack code in there today And by open source I mean where the source is available for everyone to use – mostly when made available by the authors, but also leaked source code is a pretty big deal too

- #3 1 minute Guess? So who here wants to guess what this news clip is about? Yup it's the attacks in Christmas 2015 against ukranian power stations by a group known as Sandworm. There were also attempts against Kiev's Boryspol airport and potentially the train network too, though thankfully those failed. This was a pretty big event – 250,000 people left without power on christmas eve. The power companies recovered pretty quickly by going to manual operation. Access for some time The group that did this had been gaining access to the networks for some time. They did similar attacks taking TV stations offline during Ukranian elections a few months earlier. And the US government warned about the same group over a year earlier when they found them exploring power stations in the US. The attackers tripped circuit breakers by connecting to SCADA consoles with stolen VPN credentials. It was reported the power operators could actually see the attackers taking stuff down on the SCADA screens in front of them, but they were locked out so they couldn't do anything
  https://www.eenews.net/assets/2016/07/19/document_ew_02.pdf
- #4 - 2 minutes So the group behind these are a pretty typical example of medium capability, likely state-linked attackers Custom Developed They have their own 0-days – one was for powerpoint to deliver black energy. Another was for remote access to Generel Electric SCADA software. KillDisk was used against file servers. In one case it also took out part of a SCADA system that was running Windows. Commercial Stuff In terms of commercial stuff – they used remote admin tools like teamviewer and legit tools like RDP to blend into the network BlackEnergy is the malware this group is known for – and indeed sometimes the group are just referred to as BlackEnergy Blackenergy has a really weird history, it could kind of it in any of these categories. Version 1 was commercially sold for $700 for the source code, though its now freely available. It was used in DDoS attacks in the Russia-Georgia conflict in 2008. Version 2 was commercially available again, and used by this group and others. Version 3 is used just by this group. Sandworm made great use of open source tools: Open Source ReDuh proxies tcp traffic over http – so you can run all your tools on networks with a strict firewall Weevely is a webshell Dropbear is an unfortunately named SSH server And DSE fix allows you to run unsigned drivers on Windows Tools for the job So as you might expect they use whatever tools they need for the job. They cherry pick open source tools to augment their capabilities as they need it – and that's typical of most groups that don't have the resources to custom design everything. Attribution It can also help blur the attribution. For example WannaCry has code overlaps with North Korean malware – you won't get those kinds of hints with something open source These middle capability groups have been where the growth in open source seems to be recently. Theres an Iranian group called Newscaster and a Russian group called Fancy Bear that have been using customised versions of the open source BeeF browser exploitation framework recently in watering holes. In the case of Fancy Bear that has meant using it in the place of an exploit kit that they had already built themselves They can quickly adapt the source to their needs, and operators can quickly pick up new tools when their custom main toolset is either too easily detected or attributed In contrast Low skilled attackers have always needed

free or open source software. But there is a big jump in low quality criminals taking advantage of things like open source ransomware to gain funds The danger here is they then re-invest their stolen cash into other attacks And at the other end- Another far more capable Russian group called Turla started out in the 90s using source code taken, pretty much exclusively, from Phrack magazine – but they now have their own platforms. - They do some crazy stuff with using satellite connections for command and control and other very clever things to evade detection

- #5 - 40 seconds There were follow up attacks a couple of weeks later, perhaps trying to regain lost access This time instead of their beloved blackenergy malware, they were using something called Gcat Gcat is an open source backdoor that uses gmail for command and control. Perhaps Sandworm were concerned that blackenergy was being too easily detected. Or perhaps they didn't want the targets to know it was the same people behind these later attacks. It was still obvious though as they hadn't changed their macro code that delivered the malware. The author of Gcat was understandably a little upset about this, and it's no longer developent To be clear- I'm not in anyway saying the author of Gcat is responsible for these attacks. There are plenty of rats out there to choose form and he happened to have written one that was pretty reliable -- and pretty hard to detect.
- #6 - 1 minute – Shorten this? But it does make you worry about the worst case Here are a bunch of videos on how to use freely available tools - like njRat - to hack into people's computers Now obviously there are tons of videos like this on Youtube- but what's different here is that the author claims affiliation at points to either Al Qaeda or ISIS. I'm not sure how seriously to take this guy, given he seems confused about which competing terrorist organisation he's in. But it does make you worry about the kind of worst cases. Interestingly - I think he hosted these videos on the internet archive as Youtube and Facebook took down his earlier videos In terms of how this information is shared – the internet archive is a stretched charity – they didn't have time to reply to my email about this. That's probably why the internet archive is banned in Russia for hosting terrorist content. That might also be why it was used by Russia to host the files they stole from President Macrons campaign team - during the recent french elections. Similiarly if Github started blocking open source Rats from having a home – they'd just be hosted somewhere else.
- #7 30 seconds Fast forward a year to December 2016 – and ESET reported on new attacks mostly targeting the finance sector in Ukraine By now Sandworm had re-tooled and were using a custom backdoor again. This time it looked like a Gcat inspired backdoor that instead uses Telegram for command and control They'd built their own tunneling software to replace Reduh – you can see the help file there And they'd also upgraded their KillDisk malware to leave this scary desktop background -
- #8 - 5 seconds There you are – inspired by Mr Robot apparently
- #9 15 seconds - And this is still going on– more attacks were reported this Christmas And - stock footage really is taking it to the extreme - isnt it? Not only is he wearing a hoodie in the dark – but he's also staring at a roomful of anonymous masks
- #10 - 30 seconds So Mirai is very well known – some guy wrote a worm that infects internet of things devices to build a botnet Which was then used for DDoS attacks He lots of attention after launching the biggest ever DDoS attack against Krebs – and at that point he decided to open source it I think the reason he released it onto Hackforums was probably to get some of the heat off him If a ton of script kiddies are also using your malware, it's a bit harder to tie you to a particular attack
- #11 - 30 seconds Since then someone has modified the Mirai source code added the ability to exploit some vulnerabilities in more home routers Lots of mirai attacks are still going on – someone recently use one to

try and knock malware techs WannaCry sinkhole off Interestingly there's also a worm called Hajime that is inspired by Mirai but far better built – that goes round closing security holes in internet of things devices

- #12 - 10 seconds So hidden tear is a pretty well known piece of open source ransomware I've seen a few articles on it already – so you may not know it already But I havent seen anything that covers all the ups and downs of the story
- #13 - 1 minute So it was released by Utku, who I believe was a university student at the time So you might ask – why would you create open source ransomware? He said he released it as an educational tool so people could understand how ransomware works better The disclaimer said it was for educational use only An article said it was to impress a girl – the later version called Eda was apparently named after her It was named a ransomware honeypot, and later implied it was to get bad actors to use a weak crypto implementation I think it was probably just curiosity and a bit of self publicity to get into the industry. Which I've certainly released tools for before, just with less risky consequences The code itself is pretty much what you'd expect – a few hundred lines of Visual basic that encrypts files only within one folder
- #14 - 10 seconds Some people suggested he should add a backdoor, though he chose not to And users discussing the code on Reddit pointed out a number of potential issues with the implementation of the encryption I'll go into those in a bit
- #15 10 seconds Of course - It didn't take long before real world ransomware started to take advantage of HiddenTear This was one of the first – it infected users of a website in Paraguay
- #16 - 10 seconds Utku saw the report and offered to help get the victims their files back
- #17 - 1 minute So I mentioned some issues with the implementation of the crypto in HiddenTear earlier The key is generated from the system time It uses a call to Environment.TickCount - a 32 bit integer – so it only has about 2 billion values On a modern machine that could be brute forceable in it self But the other weakness is that this value is the time that HiddenTear started. So all you need to do is get the time the first file got encrypted, within a certain window of time. So that's how Utku broke his own crypto. He attempted to decrypt a file that he knew the contents of until he'd found the key. This flaw was actually pointed out by other users, and was inspired by Bitdefender's decryption of Linux Encoder In that case it didn't work a lot of the time – because Linux Encoder is so dumb it often encrypts files in multiple rounds or simply accidentally deletes them – rendering them unrecoverable
- #18 -15 seconds After HiddenTear Utku later released an improved Most of the crypto flaws were removed – and he added features such as setting the desktop background
- #19 - 15 seconds So – lets say that you want to play Far Cry And I can it does look pretty fun, looking at this dude with antlers on his head But unfortunately you'll have to pay 39 pounds and 99 pence – that's a lot of money
- #20 -20 seconds So naturally you'll want to Google for a crack So the first result in Google when looking for a crack is this youtube video - Google makes sure that Youtube ranks well in search results And it's great that these two lovely people are going to give you Farcry for free - You can probably see where this is going
- #21 - 5 seconds But oh no – they lied Actually the crack just installs this ransomware – based on eda2
- #22 -15 seconds The worst thing about this ransomware is the ransom note the guy gives user sis really arrogant You'll never be able to find me (Voice) Even the NSA cant get your files back
- #23 - 20 seconds So Utku to the rescue again He saw users on the bleeping computer forums reporting they'd lost their files in the ransomware attack And he logged into the command and control server using a

backdoor he'd secretly left in Eda2 I've got to say – in the UK I think this might be a violation of the computer misuse act

- #24 - 25 seconds Of course it wasn't long before someone made a fork that improved on EDA2 They improved the security of the encryption and added some other features They said they made it for law enforcement… If anyone here is from law enforcement perhaps they can thank them
- #25 - 10 seconds Empinel – the author of Stolich – actually missed the backdoor in EDA2 at first but other users let them know and they then removed it
- #26 - 10 seconds So, lets say you want to play minecraft… You can probably see where this is going
- #27 - 20 seconds Oh no – it's a backdoored minecraft installer I'm not sure how to pronounce this Either Laughing My Ass Off at You? Or LmaoxUs But yeah this is based on Stolich
- #28 - 60 seconds This all happened a few months ago, but he's only removed the code from Github a couple of weeks ago Of course, forks are still available on github so the code is still available for anyone to find I was surprised when I looked into this to find the guy that forked EDA2 and wrote Stolich is only 13 years old So I give him a bit of a pass given hes only 13. Maybe when he's older he can try to stop ransomware instead, which is a much harder job. And the other point here is that stuff stays with you. The line at the bottom is a very immature - disclaimer from a password cracker I wrote ad open sourced when I was the same age as this guy I was a teenager then but all the tutorials and zines I used to write as a kid are still floating around in various places
- #30 - 10 seconds Here's a another piece of ransomware - called Magic - that is forked from EDA2
- #31 - 30 seconds The good guys took down the command and control server – but that also meant that the decryption keys were lost and the backdoor wouldnt work The malware author offered to provide a backup he had made of the keys But only if Utuk took down the source code for HiddenTear and Eda2 It isnt clear just why he wanted HiddenTear taking down, perhaps having openly available ransomware was hurting his business ____ https://www.utkusen.com/blog/project-eda2-is-abandoned-due-to-magic-ransomware-incident.html I removed all the files and commits of Eda2 project. Since nobody is discovered the backdoor of Eda2, I won't reveal it right now. Because we may deal with new Eda2 implementations in future. I'm sorry, I failed this time.
- #32 - 15 seconds So Utku took the code for them down Looking at the commit logs though, he did have enough time to upgrade the logo to EDA2 first But thankfully the attacker did give the encryption keys back so people could get their files ___ http://news.softpedia.com/news/ransomware-author-blackmails-security-researcher-who-refuses-to-give-in-499437.shtml UPDATE: After further discussions, the blackmail attempt turned into full-on negotiations, but Utku Sen and the ransomware operator have come to an agreement. Utku will take down the Hidden Tear repository in three days while the author of the Magic ransomware will provide all the encryption keys for free for the next 15 days. Victims should email the ransomware operator at viper1990@safe-mail.net.
- #33 - 25 seconds So even though the code is removed from the original Github repository – it's still available via: - The Commit history - Forks – you can see some up here -There are Improved versions too Ports – you can see one person decided to port it to C++ for some reason And also other malware inspired by the overall design decisions in HiddenTear
- #34 - 20 seconds And there have been a ton of ransomware attacks using the Hidden Tear and EDA2 code You can see here some of them…. "Don't Download Random Shit on the Internet" one says up there.. Sounds like good advice And it looks like Santa Claus is getting stoned for some reason… I dunno

- #35 -5 seconds Yep some more
- #36 - 45 seconds And more … most of these were pulled in the last couple of weeks by the way A big shout out to both Trend Micro and Bleeping Computer who reported on many of those, which saved me having to spend too long trawling through VirusTotal to find samples They are easy to find though – antivirus detections are pretty accurate and the code is easy to signature My favourite is this guy at the front – This is Microsoft Vindows Support – you have the Zeus Wirus! I tried the number by the way, it no longer works
- #37 That phone number no longer works, but this is from a newer scam that sill does, in case you'd like to talk to them
- #38 - 5 seconds This one plays the Harry potter theme tune to you
- #39 - 10 seconds This one just deletes all your files… so you cant get them back
- #40 - 15 seconds This one…. Does it look familiar? This variant came out the same time as WannaCry It's a bit like those insects that impersonate more dangerous ones so they don't get eaten
- #41 - 15 seconds You've probably heard of this one Requires you to play a weird anime game and get a certain score to get your files back Which is strange The author later apologised and released a tool to get peoples files back
- #42 - 5 seconds This one doesn't actually ask for any money, says its just to educate people about ransomware, and gives you your files back for free
- #43 - 20 seconds This one probably scares me the most – its ransomware as a service You pay $175 dollars and then you have a platform to spread ransomware from it includes a HiddenTear variant It's a very low cost entry into ransomware for criminals, and the money they make might get reinvested in more attacks
- #44 - 25 seconds So this is a great map of all the ransomware families F-Secure tagged over time I meant to highlight which ones were based on hiddentear- but it was taking too long When I was counting it was looking to be around 1 in 5, which is a pretty high amount Of course this doesn't take into account how much each variant spread So something like Locky, which is custom developed, is underrepresented here
- #45 - 25 seconds Trend Micro have some numbers – these are the unique families based on Hidden Tear that they're seeing Again this doesn't take into account how widely those families are being seen though This goes up to March – look at the samples we're getting I'd guess it's stayed pretty stable between March and May
- #46 - 20 seconds I've always found it funny seeing disclaimers like "for educational use only" As far as I can tell these mean nothing Also I've read, though I am definitely not a lawyer myself, That Open source license means you cant dictate usage And again from what I've read the Wassenaar treaty on arms control doesn't apply to open source software
- #47 - 30 seconds And finally, 2sec who these days is probably best known as Malware Tech's mate Made this poll- Do people think open source ransomware is a good thing? He got pretty much 50/50 – so as a rough show of hands Put your hands up if you think open source ransowmare is a good idea And bad? …. Anyway – so that's hiddentear
- #48 15 seconds So – the next section is mostly on leaked source code. It's not open source in the sense that there isn't a license explicitly allowing you to use the code – but then if you're deploying malware you're probably not to bothered about license anyway
- #49 - 1 minute Probably the most famous leaked code is from shadow brokers They leaked a bunch of exploits and tools allegedly stolen from the NSA This was actually taken down when first republished onto

github, from somewhere else And it wasn't taken down because of the exploits It was taken down because they included the auction message from the shadow brokers – and you're not allowed to ask for cash on Github To be fair Github has got a pretty hard job deciding what to allow or not For example they don't allow compiled malware But they do allow you to host scripts that can you can run as is So I've seen on incident response jobs, attackers running powershell mimikatz straight off of github.com And that's a pain to detect at the network level without ssl terminators So you just see an encrypted connection to Github.com Its also a pain to stop with application whitelisting as it's not an executable though there's plenty you can do to detect malicious powershell usage

- #50 - 50 seconds One of these exploits is EternalBlue – the SMB version 1 exploit made famous by its abuse in WannaCry The exploit was leaked back in April, and some people were playing with it when it came out But WannaCry didn't happen until a month after those exploits were released An analysis by BAE showed that WannaCry used an easier to use version of the exploit - Developed just a couple of days before WannaCry spread to Github If they hadn't released this version of the exploit – would WannaCry have still happened? And now its in metasploit… And whenever things end up in metasploit – you quickly see that code being reused in malware
- #51 - 80 seconds This is leaked source code from Fancy bear or APT28 Funnily enough there's a good chance these are the same guys behind Shadow Brokers, - So what goes around - comes around They left two of their command and control servers open so anyone could grab the source code Also in terms of sharing is caring A journalist leaked the analysis that one of the security guys at Google had done on this malware And that's a whole other side of sharing is caring – on the defensive side- that I don't have time to cover in this talk The product that I work on, OTX, we have problems with getting the sharing right. We really want users to share information on attacks there, but we've also had plenty of cases of people using our platform to leak vendors private threat intelligence reports And some of that is pretty sensitive- both commercially because we don't want people stealing other peoples intellectual property But more importantly because if attackers see there's a private report on their malware, clearly they will change how they operate and then we won't be able to detect them anymore ___ Journalist leaked Google report – sharing is caring – tlp amber
- #52 - 45 seconds Hacking team are a very controversial surveillance company They sell exploits and malware to law enforcement But they also have a habit of not only selling to regimes that would use it for things like counter terrorism, but also to places where they use it against dissidents and journalists that criticse the government So someone hacked them and put all their stuff on Github… The exploits were used almost immediately Pirated versions of HackingTeams malware has been seen in targeted attacks by Russian nationalists. They're quite a low capability group but pretty dangerous When Putin talks about nationalist hackers it could be these guys he means – but these aren't the group that are impacting elections
- #53 - 50 seconds Shadowserver did a really nice analysis of how two of the Hacking team leaked exploits were packaged up and used by some groups based in China It looks like there was one central development shop - or quartermaster, that packaged up the exploits then shared them with various other China based groups And this is something you see a lot with targeted attacks I saw something similar when looking at groups that used a Chinese exploit framework, which is a frankenstein of various open source bits of code, and is distributed from one central development shop
- #54 - 35 seconds So Carberp was a banking trojan that made many millions of pounds a few years ago It was built by about 25 programmers who all worked remotely, they were paid a couple of thousand dollars

to write modules to extend the trojan Most worked around the black sea, which is a hot bed for this kind of high end cyber crime It's always interesting to see whose behind a big operation like this – you can see one of the ringleaders getting arrested here -hes not having a good day He lives in Moscow and made the mistake of targeting a ton of Russian banks And what happened after these guys were arrested is pretty much the same as what happened with the Zeus banking malware The code was soon being sold on forums by people who had access, and finally it got leaked enough it was freely available ___ Show video from https://life.ru/t/%D0%BD%D0%BE%D0%B2%D0%BE%D1%81%D1%82%D0%B8/86143 Summarise https://krebsonsecurity.com/tag/carberp/ https://www.welivesecurity.com/2012/07/02/all-carberp-botnet-organizers-arrested/ http://translate.google.com/translate?sl=ru&tl=en&js=n&prev=_t&hl=en&ie=UTF-8&eotf=1&u=http%3A%2F%2Fwww.kommersant.ua%2Fdoc%2F2160535&act=url&act=url&act=url

- #55 2 minutes And it seems that everyone uses Carberp! Both Carberp and Zeus are used as the basis for most banking malware sold on forums today - To the extent that people selling malware advertise if their malware isn't based on Zeus and Carberp – because they are now so easy to detect Sofacy or APT28 use it in some of their code, together with Metasploit - They are a very well resourced organisation, but it makes sense for them to develop as quickly as possible given they have a remit to hack thousands of people every year It was pretty well reported on that Wikileaks leaked what is apparently CIA tools and malware recently One of the things in that massive dump is a backdoor which uses parts of Carberp Its nice to see them saving tax payer money They also say that they've carefully vetted the code for vulnerabilities and backdoors, which is quite hard to do The quote here comments that making Carberp, which previously cost $40k, available to everyone is like "handing a bazooka to a child" - Which makes you wonder what the comparison would be for making entire NSA and CIA entire platforms, worth many millions of pounds, freely available is like Maybe its more like handing a nuke to a child, and that's why we have things like WannaCry
- #56 - 10 seconds So are there some upsides to all this open source malware and leaked code being available to anyone?
- #57 - 15 seconds As mentioned earlier, when everyone bases their malware on the same code base it can make it easier to detect Most HiddenTear variants are detected pretty trivially as HiddenTear There are packers and obfuscators though that can make the job more difficult
- #58 - 40 seconds For one thing having the source code for Carberp made it easier to find vulnerabilties And looking at it some of the code is actually pretty terrible So it didn't take long before researchers found they could remotely take control of Carberp command and control servers And whilst people can fork Carberp and fix these holes – I havent seen anyone do it. I guess it's hard to get the many eyes advantages of open source when there's not a central active developer for leaked code So up here on the screen are some command and control servers that Xylitol took over
- #59 10 - And finally I didn't have space on the slides to thank everyone whose screenshots and research I used, so many thanks to them
- #60 20 - So – that's it Any questions?
