MalwareTech

Malware Reversing News Contact Botnet Tracker
Text to Search...

How to Accidentally Stop a Global Cyber Attacks

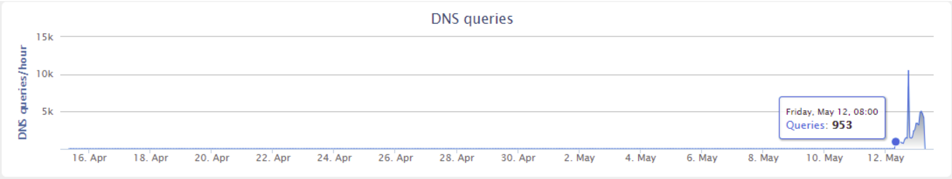
May 13, 2017 MalwareTech ms17-010, ransowmare, worm 183

So finally I've found enough time between emails and Skype calls to write up on the crazy events which occurred over Friday, which was supposed to be part of my week off (I made it a total of 4 days without working, so there's that). You've probably read about the WannaCrypt fiasco on several news sites, but I figured I'd tell my story.

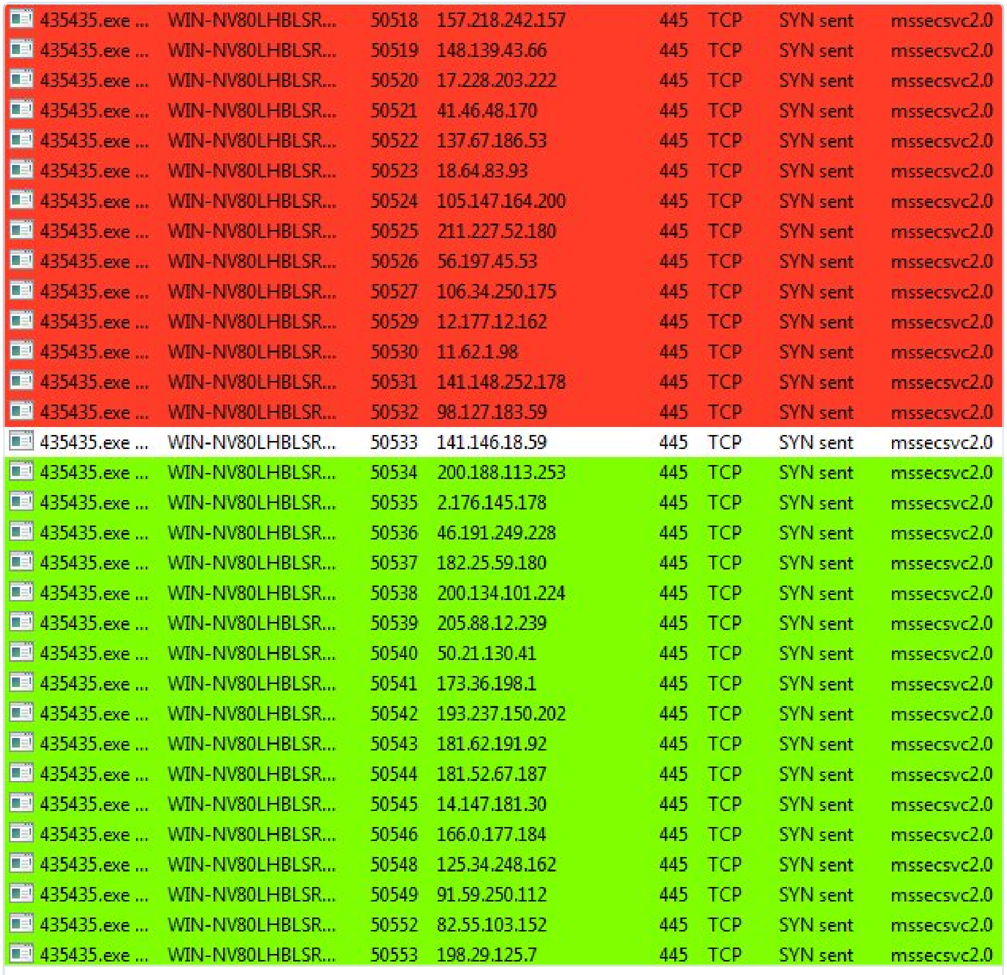
I woke up at around 10 AM and checked onto the UK cyber threat sharing platform where i had been following the spread of the Emotet banking malware, something which seemed incredibly significant until today. There were a few of your usual posts about various organisations being hit with ransomware, but nothing significant…yet. I ended up going out to lunch with a friend, meanwhile the WannaCrypt ransomware campaign had entered full swing.

When I returned home at about 2:30, the threat sharing platform was flooded with posts about various NHS systems all across the country being hit, which was what tipped me of to the fact this was something big. Although ransomware on a public sector system isn't even newsworthy, systems being hit simultaneously across the country is (contrary to popular belief, most NHS employees don't open phishing emails which suggested that something to be this widespread it would have to be propagated using another method). I was quickly able to get a sample of the malware with the help of Kafeine, a good friend and fellow researcher. Upon running the sample in my analysis environment I instantly noticed it queried an unregistered domain, which i promptly registered.

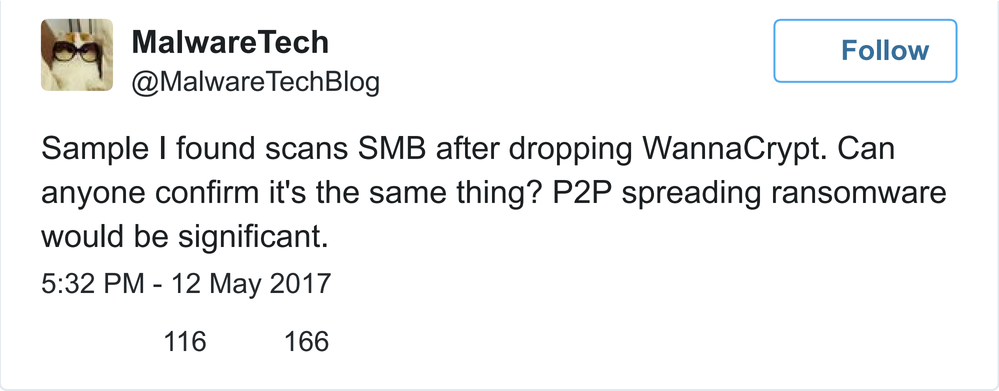
Using Cisco Umbrella, we can actually see query volume to the domain prior to my registration of it which shows the campaign started at around 8 AM UTC.



While the domain was propagating, I ran the sample again in my virtual environment to be met with WannaCrypt ransom page; but more interestingly was that after encrypting the fake files I left there as a test, it started connecting out to random IP addresses on port 445 (used by SMB). The mass connection attempts immediately made me think exploit scanner, and the fact it was scanning on the SMB port caused me to look back to the recent ShadowBroker leak of NSA exploits containing….an SMB exploit. Obvious I had no evidence yet that it was definitely scanning SMB hosts or using the leaked NSA exploit, so I tweeted out my finding and went to tend to the now propagated domain.



435435.exe ...	WIN-NV80LHBLSR...	50518	157.218.242.157	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50519	148.139.43.66	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50520	17.228.203.222	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50521	41.46.48.170	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50522	137.67.186.53	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50523	18.64.83.93	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50524	105.147.164.200	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50525	211.227.52.180	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50526	56.197.45.53	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50527	106.34.250.175	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50529	12.177.12.162	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50530	11.62.1.98	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50531	141.148.252.178	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50532	98.127.183.59	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50533	141.146.18.59	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50534	200.188.113.253	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50535	2.176.145.178	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50536	46.191.249.228	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50537	182.25.59.180	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50538	200.134.101.224	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50539	205.88.12.239	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50540	50.21.130.41	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50541	173.36.198.1	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50542	193.237.150.202	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50543	181.62.191.92	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50544	181.52.67.187	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50545	14.147.181.30	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50546	166.0.177.184	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50548	125.34.248.162	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50549	91.59.250.112	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50552	82.55.103.152	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50553	198.29.125.7	445	TCP	SYN sent	mssecsvc2.0



MalwareTech
@MalwareTechBlog

Sample I found scans SMB after dropping WannaCrypt. Can anyone confirm it's the same thing? P2P spreading ransomware would be significant.

5:32 PM - 12 May 2017

116 166

Now one thing that’s important to note is the actual registration of the domain was not on a whim. My job is to look for ways we can track and potentially stop botnets (and other kinds of malware), so I’m always on the lookout to pick up unregistered malware control server (C2) domains. In fact I registered several thousand of such domains in the past year.

Our standard model goes something like this.

1. Look for unregistered or expired C2 domains belonging to active botnets and point it to our sinkhole (a sinkhole is a server designed to capture malicious traffic and prevent control of infected computers by the criminals who infected them).
2. Gather data on the geographical distribution and scale of the infections, including IP addresses, which can be used to notify victims that they’re infected and assist law enforcement.
3. Reverse engineer the malware and see if there are any vulnerabilities in the code which would allow us to take-over the malware/botnet and prevent the spread or malicious use, via the domain we registered.

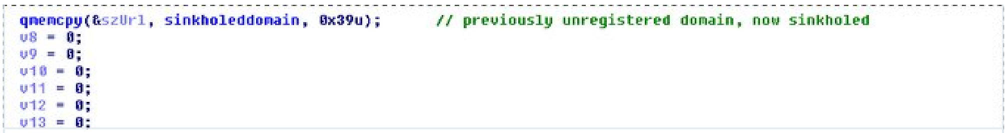
In the case of WannaCrypt, step 1, 2 and 3 were all one and the same, I just didn’t know it yet.

A few seconds after the domain had gone live I received a DM from a Talos analyst asking for the sample I had which was scanning SMB host, which i provided. Humorously at this point we had unknowingly killed the malware so there was much confusion as to why he could not run the exact same sample I just ran and get any results at all. As curious as this was, I was pressed for time and wasn’t able to investigate, because now the sinkhole servers were coming dangerously close to their maximum load.

I set about making sure our sinkhole server were stable and getting the expected data from the domain we had registered (at this point we still didn't know much about what the domain I registered was for, just that anyone infected with this malware would connect to the domain we now own, allowing us to track the spread of the infection). Sorting out the sinkholes took longer than expected due to a very large botnet we had sinkholed the previous week eating up all the bandwidth, but soon enough I was able to set up a live tracking map and push it out via twitter (you can still see it here).

Around 6:23 PM (BST) I asked an employee to look into the worm code and verify the domain we registered would not change (some malware will periodically change the domain using an algorithm, so we needed to know if there would be new domains so we could register those too), meanwhile I performed some updated to the live map to deal with the rapid influx of new visitors.

After about 5 minutes the employee came back with the news that the registration of the domain had triggered the ransomware meaning we'd encrypted everyone's files (don't worry, this was later proven to not be the case), but it still caused quite a bit of panic. I contacted Kafeine about this and he linked me to the following freshly posted tweet made by ProofPoint researcher Darien Huss, who stated the opposite (that our registration of the domain had actually stopped the ransomware and prevent the spread).



```
qmemcpy(&szUrl, sinkholeddomain, 0x39u);      // previously unregistered domain, now sinkholed
v8 = 0;
v9 = 0;
v10 = 0;
v11 = 0;
v12 = 0;
v13 = 0;
```

Darien Huss
@darienhuss

Follow

#WannaCry propagation payload contains previously unregistered domain, execution fails now that domain has been sinkholed

7:29 PM - 12 May 2017

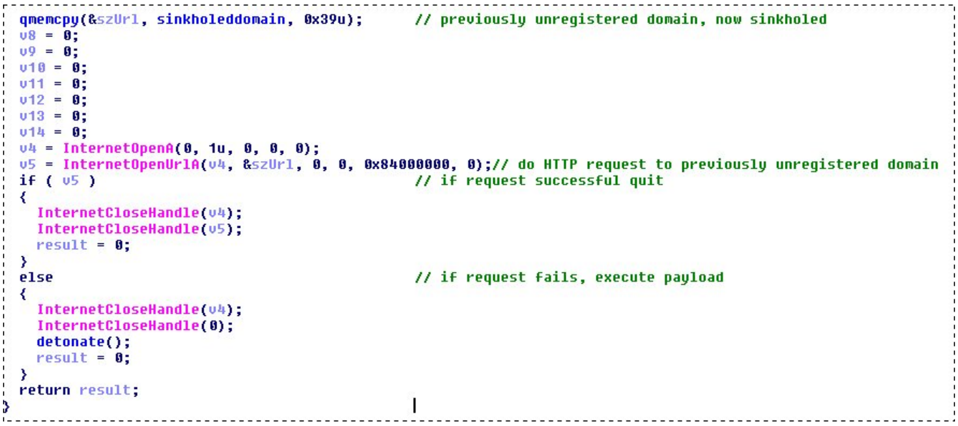
1,142 1,634

Having heard to conflicting answers, I anxiously loaded back up my analysis environment and ran the sample….nothing. I then modified my host file so that the domain connection would be unsuccessful and ran it again…..RANSOMWARED.

Now you probably can't picture a grown man jumping around with the excitement of having just been ransomwared, but this was me. The failure of the ransomware to run the first time and then the subsequent success on the second mean that we had in fact prevented the spread of the ransomware and prevented it ransoming any new computer since the registration of the domain (I initially kept quiet about this while i reverse engineered the code myself to triple check this was the case, but by now Darien's tweet had gotten a lot of traction).

So why did our sinkhole cause an international ransomware epidemic to stop?

Talos wrote a great writeup explaining the code side here, which I'll elaborate on using Darien's screenshot.



```
qmemcpy(&szUrl, sinkholeddomain, 0x39u);      // previously unregistered domain, now sinkholed
v8 = 0;
v9 = 0;
v10 = 0;
v11 = 0;
v12 = 0;
v13 = 0;
v14 = 0;
v4 = InternetOpenA(0, 1u, 0, 0, 0);
v5 = InternetOpenUrlA(v4, &szUrl, 0, 0, 0x84000000, 0);// do HTTP request to previously unregistered domain
if ( v5 )                                     // if request successful quit
{
  InternetCloseHandle(v4);
  InternetCloseHandle(v5);
  result = 0;
}
else                                          // if request fails, execute payload
{
  InternetCloseHandle(v4);
  InternetCloseHandle(0);
  detonate();
  result = 0;
}
return result;
}
```

All this code is doing is attempting to connect to the domain we registered and if the connection is not successful it ransoms the system, if it is successful the malware exits (this was not clear to me at first from the screenshot as I lacked the context of what the parent function may be doing with the results).

The reason which was suggested is that the domain is a “kill switch” in case something goes wrong, but I now believe it to be a badly thought out anti-analysis.

In certain sandbox environments traffic is intercepted by replying to all URL lookups with an IP address belonging to the sandbox rather than the real IP address the URL points to, a side effect of this is if an unregistered domain is queried it will respond as it it were registered (which should never happen).

I believe they were trying to query an intentionally unregistered domain which would appear registered in certain sandbox environments, then once they see the domain responding, they know they’re in a sandbox the malware exits to prevent further analysis. This technique isn’t unprecedented and is actually used by the Necurs trojan (they will query 5 totally random domains and if they all return the same IP, it will exit); however, because WannaCrypt used a single hardcoded domain, my registartion of it caused all infections globally to believe they were inside a sandbox and exit…thus we initially unintentionally prevented the spread and and further ransoming of computers infected with this malware. Of course now that we are aware of this, we will continue to host the domain to prevent any further infections from this sample.

One thing that is very important to note is our sinkholing only stops this sample and there is nothing stopping them removing the domain check and trying again, so it’s incredibly importiant that any unpatched systems are patched as quickly as possible.

As well as the names & companies mentioned in this blog I’d like to give a shout out to:

NCSC UK – Their threat intelligence sharing program provided us with valuable information needed to first identify the malware family behind the attack. They also helped ensure our sinkholes were not mistaken for criminal controlled infrastructure so that we could feed them the information required to notify UK victims.

FBI & ShadowServer – They were a great help in getting non-UK victims notified of the infections in a very short span of time, even if it did mean me staying up all night to link in with them.

2sec4u – For reducing my workload today and providing free panic attacks.

Microsoft – By realeasing an out of bounds patch for unsupported operating systems such as Windows XP and Server 2003, people now are able to patch rather than having to attempt upgrades to newer system in order to be secured against this worm.

If you have anything to patch, patch it. If you need a guide, this one is being reguarly updated: https://www.ncsc.gov.uk/guidance/protecting-your-organisation-ransomware

Now I should probably sleep.

181 Comments **malwaretech2** 1 **Login**

♡ **Recommend** 190 **Share** **Sort by Best**

Join the discussion…

Michael Mudd • 20 hours ago
The media are dead wrong calling you an 'Accidental Hero', you are a professional and this was great work, well done!
190 ^ | ˅ • Reply • Share ›

Derrick James ➦ Michael Mudd • 19 hours ago
he titled the article as "accident" so.....it's not the media's fault
8 ^ | ˅ • Reply • Share ›

greggreen29 ➦ Derrick James • 18 hours ago
It does demonstrate how many reporters and editors are technically and comprehensively illiterate.

"My job is to look for ways we can track and potentially stop botnets..."

"I was quickly able to get a sample of the malware with the help of Kafeine, a good friend and fellow researcher."

the help of Kafeine, a good friend and fellow researcher.

"Upon running the sample in my analysis environment I instantly noticed it queried an unregistered domain, which i promptly registered."

None of these events were accidental.

25 ^ | ˅ • Reply • Share ›

Aris Adamantiadis ➦ greggreen29 • 17 hours ago

To be fair, he said himself he thought at some point that registering the domain name triggered the ransomware instead of disabling it. The story headline would have mentioned "Security research accidentally armed a ransomware" in that case. His experience told him it was a good thing to own domains used by C&C, his luck made it that it was a kill switch. I don't think "accidental" is undeserved in this case.
Whatever, it's good job!

5 ^ | ˅ • Reply • Share ›

Greg Martin ➦ Aris Adamantiadis • 13 hours ago

I think it's an unconscious assumption that the writer of the article is male. I've gotten better over time at noticing such implicit bias within myself, but we still fall into that trap sometimes.

1 ^ | ˅ • Reply • Share ›

Michael ➦ Greg Martin • 12 hours ago

Well, the bit where he says to picture a grown man jumping around was a clue for me.

I wasn't unconscious when I read it though maybe that helped

5 ^ | ˅ • Reply • Share ›

Thistle_Weed2 ✓verɪfɪed Trump ➦ Greg Martin
• 10 hours ago

re; 'implicit bias' triggered?

men use less words to convey an idea than females, it's how our brains (srs- it's like proven via research etc, go on and google it) work. I completely read this as male author. As a female who works low level tech for nearly 19 yrs, I have no problem assuming it's a male. Working women in tech don't give 2 flips about male/female. So Greg, be a dear and don't defend women. We can do that ourselves. keep your coat on and don't worry about any rain puddles and helping us...

m'kay?

1 ^ | ⌄ • Reply • Share ›

Longtime_Geek ➦ Thistle_Weed2 ✓verɪfɪed Trump • 3 hours ago

"be a dear and don't defend women. We can do that ourselves"

Belittling, however kindly, those that support gender equality simply because they happen to be male, is to fall victim to the very behavior you fight against. That behavior is often called sexism, and you exhibited exactly that by condescending to men as if they can't possibly feel as you do.

Be a dear and don't criticize men who believe as you do, that all human beings deserve the same rights, regardless of gender.

1 ^ | ⌄ • Reply • Share ›

Dave ➦ greggreen29 • 17 hours ago

The media is filled with people who don't do their research. This is both true in the IT world along with the firearms world. Me being involved in both. Media however LOVES buzzwords without even knowing what that word means nor use it in context correctly.

They make conclusions about things they don't even understand or refer to a real expert in the field or multiple to get out of single sourced subjective analysis problems.

I am no total expert in either though I do know a lot, but I make my due diligience if I do write aboit a subject, I do RESEARCH vs WEBSEARCH on it to draw conclusions. I also then employ logic and personal experiences for supplimenting those conclusions if I have the experiences to draw upon.

This is why I follow people I would deem as experts in the field, to learn more about what we come across, to ask questions, and to constantly learn.

This is why I follow the Malwaretech crew and others like them in security and forensics.

Malwaretech, thank you for your service, not only for this incident, but all the research you do.

4 ^ | ⌄ • Reply • Share ›

4 ^ | ⌄ • Reply • Share ›

Susan O'neill ➦ Dave • 15 hours ago

Well said Dave. Whilst I struggled to follow the report on his progress, it would seem that he is connected to people who can offer a service and using his own expertise and by a process of elimination, find the answers, but because he caught on to something very quickly(which he might easily have missed, had he not been so thorough and alert)would have allowed the worm to continue it's travels. I think a lot of people should be very thankful to MalwareTech and his expertise - even if it does generate more business for him, it's probably well deserved.

1 ^ | ⌄ • Reply • Share ›

Susan O'neill ➦ greggreen29 • 15 hours ago

I assume you mean his MO in tracking and identifying any miscreant doings was deliberate, but he does state that it was his good fortune in triggering a default response which in a way, is as he stated - accidental, as opposed to deliberate.

2 ^ | ⌄ • Reply • Share ›

Michael ➦ greggreen29 • 12 hours ago

Well of course.

The accident was the (at the time) unknown consequences of registering the domain which happened to be fortuitous.

^ | ⌄ • Reply • Share ›

Mike K ➦ Michael Mudd • 19 hours ago

AGREED! Accident my @$s. Nicely done.

3 ^ | ⌄ • Reply • Share ›

motrek ➦ Mike K • 15 hours ago

Of course it was an accident. When he registered the domain, he didn't think "hey, this'll stop the worm!" Hence accident.

^ | ⌄ • Reply • Share ›

mawelsh ➦ motrek • 11 hours ago

3 ^ | v • Reply • Share ›

Greg Martin ➦ motrek • 13 hours ago

I think it's an unconscious assumption that the writer of the article is male. I've gotten better over time at noticing such implicit bias within myself, but we still fall into that trap sometimes....

^ | v • Reply • Share ›

Michael ➦ Greg Martin • 12 hours ago

Well, no, it's a simple case of reading the article carefully and noting that he says his gender

2 ^ | v • Reply • Share ›

Thistle_Weed2 ✓verɪfɪed Trump ➦ Greg Martin • 10 hours ago

/facepam

as a women, I say please shut up. beyond silly bringing that gender nonsense into a serious conversation and frankly insulting.

1 ^ | v • Reply • Share ›

Daniel ➦ Greg Martin • 8 hours ago

"Now you probably can’t picture a grown man jumping around with the excitement of having just been ransomwared, but this was me."

^ | v • Reply • Share ›

DanHess00 ➦ Greg Martin • 9 hours ago

Implicit bias? Trap? Yes, indeed, comrade, what you did was serious. I will have recommend you for reeducation camp. It is for your own good.

^ | v • Reply • Share ›

Jon Du Puy ➦ Michael Mudd • 6 hours ago

WELL PUT!!!! AQND YES CONGRATULATIONS MalwareTech!!!!! 6 STARS!!!!

LONG LIVE THE SINK HOLE--- HOPE YOU GOT THAT WELL DESERVED SLEEP. CHEERS

^ | v • Reply • Share ›

motrek ➦ Michael Mudd • 15 hours ago

The "accident" is that an action the author took had an unintended effect. In this case the effect was desirable (a happy accident), but if it wasn't, nobody would be arguing about the use of the word "accident."

It might not be the ideal word for what happened but I'm struggling to think of a better one.

⌃ | ⌄ • Reply • Share ›

GreatLakeSailor ➦ motrek • 13 hours ago

serendipitous

⌃ | ⌄ • Reply • Share ›

greggreen29 ➦ Michael Mudd • 18 hours ago

I can't believe how stupid journalists are. "My job is to look for ways we can track and potentially stop botnets..."

Maybe journalists are so technically deficient that everything involving PCs is accidental.

⌃ | ⌄ • Reply • Share ›

Toddddds • 19 hours ago

This outcome was a direct result of your extraordinary efforts and obvious long term experience. Your competence and dedication is a credit to yourself, your company and IT pros everywhere. The media, since they are only good for parroting, can't fathom a creative individual making a difference, so they belittle your contribution as "accidental." All discoveries are accidental, and the result of diligent efforts such as yours. It's not like you logged onto Facebook and accidentally discovered the answer while browsing cat pictures. I've never heard of your blog before today and will be paying attention to your missives as this is news I can use in support of my clients. Thank you.

17 ⌃ | ⌄ • Reply • Share ›

TheBeholder ➦ Toddddds • 17 hours ago

“Luck is what happens when preparation meets opportunity" Seneca

5 ⌃ | ⌄ • Reply • Share ›

pyronite ➦ Toddddds • 12 hours ago

Please don't take this opportunity to push your own anti-media narrative. MalwareTech himself portrays this as accidental:

1 ^ | v • Reply • Share ›

Psyclon • 19 hours ago

Read from this great find in a German newspaper.
I think "accidently" is totally wrong since you looked into the code, set up the environments, did tests etc.

I like this read. Not being a professional (more an "advanced user") many of those blogs are just too much for me. This one was a pleasure and understandable for every non-programmer!

8 ^ | v • Reply • Share ›

Adam Dunlop • 20 hours ago

Thank you for your great work to stop this attack. How many hits on the domain now?

7 ^ | v • Reply • Share ›

Jeff Bouchard • 17 hours ago

Needless to say well done!
and this kind if instinct is no accident

see more

6 ^ | v • Reply • Share ›

Norman McIlwain • 16 hours ago

You haven't exactly saved the world, but it feels like it. :)

4 ^ | v • Reply • Share ›

Asdrubal Trombone • 17 hours ago

I understand when highly skilled professionals would be humble enough to not be seen as arrogant or selfish about their achievements. It is obvious the word "accidentally" is not the right word to be used but the reading of your article is enough to let us know a lot about the professionalism and character of the author. Very well done, sir. Cheers professionalism and character of the author. Very well done, sir. Cheers from Brazil!

4 ⌃ | ⌄ • Reply • Share ›

BassieB • 17 hours ago

Someone pay the man.

4 ⌃ | ⌄ • Reply • Share ›

dbe4876 • 18 hours ago

Not my world, but fascinating read, and glad there are folks like you (and your community) out there in the battle! Thank you!

4 ⌃ | ⌄ • Reply • Share ›

thuo63 • 20 hours ago

You is got skills blud. Respect.

4 ⌃ | ⌄ • Reply • Share ›

John Steel • 20 hours ago

Nice job! Thanks for the write up. :)

4 ⌃ | ⌄ • Reply • Share ›

Laurie Robinson • 20 hours ago

Great work and write up, thanks!!

4 ⌃ | ⌄ • Reply • Share ›

Richard • 13 hours ago

Google Plus

MalwareTech

google.com/+MalwaretechNetwork

Malware Analysis, Security News, Reverse Engineering.

Folgen +1

+ 577

Archives

- ▶ 2017 (3)
- ▶ 2016 (18)
- ▶ 2015 (26)
- ▶ 2014 (26)
- ▶ 2013 (18)