INFOSEC

Topics / Hacking / **Hacking Tor and Online Anonymity**

Hacking

Hacking Tor and Online Anonymity

August 6, 2014 by **Pierluigi Paganini**

Share:

Introduction

Tor is the acronym of "The onion router", a system implemented to preserve online anonymity. Tor client software routes Internet traffic through a worldwide volunteer network of servers that hide user information, eluding surveillance of government and other bad actors.

The Tor project was born in the military sector, sponsored the US Naval Research Laboratory, and from 2004 to 2005 it was supported by the Electronic Frontier Foundation. Today the software is under development and maintenance of the Tor Project Team.

In this Series

Hacking Tor and Online Anonymity

How to hack mobile communications via Unisoc baseband vulnerability

How to build a hook syscall detector

Top tools for password-spraying attacks in active directory networks

NPK: Free tool to crack password hashes with AWS

Tutorial: How to exfiltrate or execute files in compromised machines with DNS

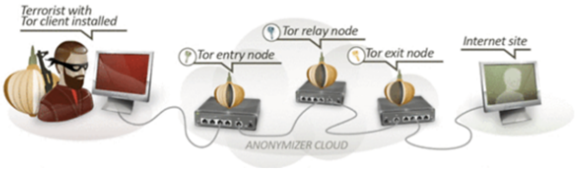
Top 19 tools for hardware hacking with Kali Linux

20 popular wireless hacking tools [updated 2021]

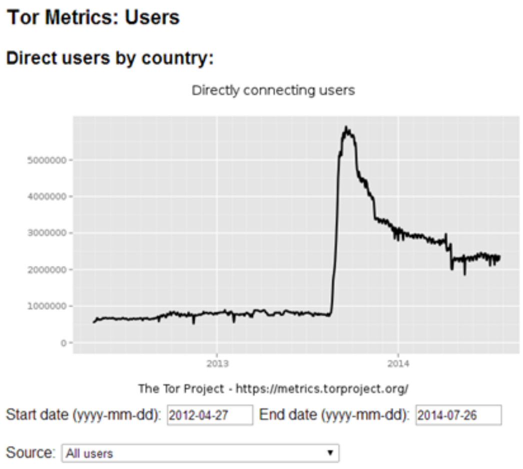
13 popular wireless hacking tools [updated 2021]

Man-in-the-middle attack: Real-life example and video walkthrough [Updated 2021]

The encryption processes implemented in the Tor Network allow it to protect users' privacy. Tor traffic is encrypted multiple times passing through different nodes of the network, also known as Tor relays.



Law enforcement and Intelligence agencies all over the world are spending a considerable effort to try to break the encryption used with Tor. Practically every government is trying to infiltrate the network to de-anonymize its users. The Tor network is widely used by digital activists and individuals in many critical regions to avoid the Internet censorship operated by governments in China, Syria, Bahrain and Iran. According to Tor Metrics, the number of people worldwide who directly access the anonymizing network is 2.5 million.



Tor Metrics: Users

Direct users by country:

The Tor Project - https://metrics.torproject.org/

Start date (yyyy-mm-dd): 2012-04-27 End date (yyyy-mm-dd): 2014-07-26

Source: All users ▾

Figure – Users directly connected to Tor network

In this post is an overview of the recent events regarding Tor and the attacks on its infrastructures, with explicit reference to principal initiatives conducted by governments to de-anonymize Tor users.

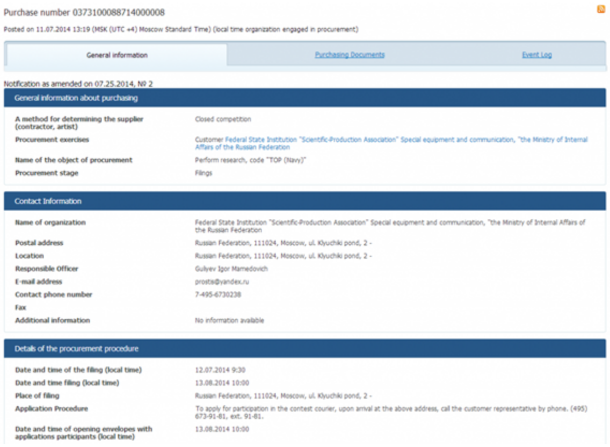
Governments vs Tor

Governments are spending great effort to improve monitoring capabilities. Tor networks and other anonymizing networks represent an obstacle to Internet monitoring. Governments sustain that technologies like Tor are abused by cybercrime and terrorists and are a potential source of threats, but organizations for the defense of online privacy and freedom of expression sustain that intelligence agencies are trying to extend their monitoring capabilities over anonymizing networks.

Russian Government wants to crack Tor

Intelligence agencies declared war on the anonymizing network. Edward Snowden revealed months ago that the US intelligence is worried by possible misuses of the Tor network and was investing to compromise it. Also the Russian government is actively working to try to crack Tor encryption to de-anonymize its users. The Ministry of the Interior of the Russian Federation (MVD) has recently started an initiative to “study the possibility of obtaining technical information about users (user equipment) of Tor anonymous network”.

The Russian government has issued a tender to recruit companies and organizations which are interested in developing the technology to track users and their activities within the Tor network. The authorities are offering nearly 4 million rubles, approximately $111,000, for the development of technology to decrypt data sent over Tor and identify Tor users. The tender, titled “Perform research, code ‘TOR’ (Navy),” was posted on July 11th on the official procurement website.



Purchase number 0373100088714000008

Posted on 11.07.2014 13:19 (MSK (UTC +4) Moscow Standard Time) (local time organization engaged in procurement)

Notification as amended on 07.25.2014, № 2

General information about purchasing

A method for determining the supplier (contractor, artist)	Closed competition
Procurement exercises	Customer Federal State Institution "Scientific-Production Association" Special equipment and communication, "the Ministry of Internal Affairs of the Russian Federation
Name of the object of procurement	Perform research, code "TOP (Navy)"
Procurement stage	Filings

Contact Information

Name of organization	Federal State Institution "Scientific-Production Association" Special equipment and communication, "the Ministry of Internal Affairs of the Russian Federation
Postal address	Russian Federation, 111024, Moscow, ul. Klyuchiki pond, 2 -
Location	Russian Federation, 111024, Moscow, ul. Klyuchiki pond, 2 -
Responsible Officer	Gulyev Igor Mamedovich
E-mail address	prosts@yandex.ru
Contact phone number	7-495-6730238
Fax	
Additional information	No information available

Details of the procurement procedure

Date and time of the filing (local time)	12.07.2014 9:30
Date and time filing (local time)	13.08.2014 10:00
Place of filing	Russian Federation, 111024, Moscow, ul. Klyuchiki pond, 2 -
Application Procedure	To apply for participation in the contest courier, upon arrival at the above address, call the customer representative by phone. (495) 673-91-81, ext. 91-81.
Date and time of opening envelopes with applications participants (local time)	13.08.2014 10:00

Figure – Competition promoted by the Ministry of the Interior of the Russian Federation (MVD)

Officially the Kremlin is sustaining similar projects “in order to ensure the country’s defense and security”. Russian intelligence fears that the anonymizing networks could be used by terrorists and foreign intelligence to conspire against the government of Moscow. A few days ago I asked a colleague to help me to translate the original tender, the spelling of “TOP” comes from that original document (all-caps, Russian transliteration). The tender is about Tor indeed and the term “Scientific Production Association” (Научно -производственное Объединение) is a Soviet/Russian cover word for a military or a KGB/FSB R&D outlet. The one in question belongs to the Interior Ministry, which is in charge of police and penitentiary.

The tender requires active security clearance specifically in the LI (though I wonder if “legal” is applicable to Russia at all) and a general high level security clearance.

Every company that desires to participate in the initiative has to pay a 195,000 ruble (about $5,555) application fee.

Who is spying on Tor network exit nodes from Russia?

The researchers Philipp Winter and Stefan Lindskog of Karlstad University in Sweden presented the results of a four-month study conducted to test Tor network exit nodes for sneaky behavior. The expert noticed that a not-specified Russian entity is eavesdropping on nodes at the edge of the Tor network.

The principle on which their investigation is based is the possibility to monitor for exit relays to snoop and tamper with anonymized network traffic. The researchers have worked to define a methodology to expose malicious exit relays and document their actions. The researchers used a custom tool, a “fast and modular exit relay scanner”, for their analysis, and they discovered that the entity appeared to be particularly interested in users’ Facebook traffic.

They designed several scanning modules for detecting common attacks and used them to probe all exit relays.

“We are able to detect and thwart many man-in-the-middle attacks which makes the network safer for its users,” they reported in the paper published in their research.

Winter and Lindskog identified 25 nodes that tampered with web traffic, decrypted the traffic, or censored websites. On the overall nodes compromised, 19 were tampered with using a man-in-the-middle attacks on users, decrypting and re-encrypting traffic on the fly.

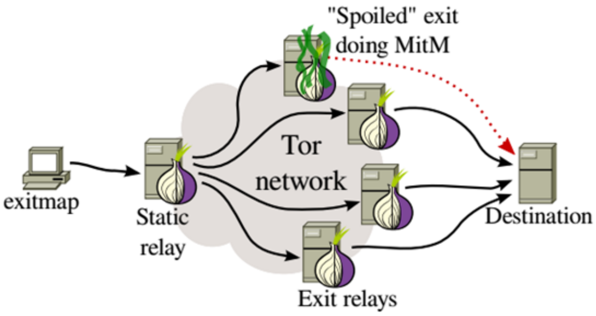


Figure – Tor network infiltrated by malicious nodes

Tor network anonymizes users' web experience, under specific conditions, bouncing encrypted traffic through a series of nodes before accessing the web site through any of over 1,000 "exit nodes."

The study proposed is based on two fundamental considerations:

- User's traffic is vulnerable at the exit nodes. For bad actors, the transit through an exit node of the traffic exposes it to eavesdropping. The case of WikiLeaks was very popular, which was initially launched with documents intercepted from the Tor network eavesdropping on Chinese hackers through a bugged exit node.
- Tor nodes are run by volunteers that can easily set up and take down their servers every time they need and want.

The attackers in these cases adopted a bogus digital certificate to access the traffic content. For the remaining six cases, it has been observed that impairment resulted from configuration mistakes or ISP issues.

The study revealed that the nodes used to tamper the traffic were configured to intercept only data streams for specific websites, including Facebook, probably to avoid detection of their activity.

The researchers passive eavesdropped on unencrypted web traffic on the exit nodes. By checking the digital certificates used over Tor connections against the certificates used in direct “clear-web sessions”, they discovered numerous exit nodes located in Russia that were used to perform man-in-the-middle attacks.

The attackers control the Russian node access to the traffic and re-encrypt it with their own self-signed digital certificate issued to the made-up entity “Main Authority.”

It is difficult to attribute the responsibility for these attacks. Researchers speculated the attacks are part of a sophisticated operation conducted to de-anonymize the Tor network. The experts also noticed that when blacklisting the “Main Authority” Tor nodes, new ones using the same certificate would be setup by the same entity.

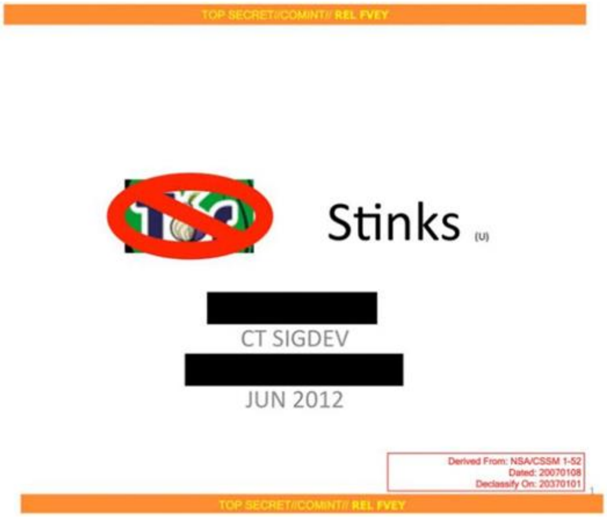
The experts exclude that any government agency was conducting the attack because the technique adopted is too noisy. They suspect that a group of isolating individuals is responsible for the anomalous activity. One of the most noisy choices of the attackers is the use of self-signed certificates that cause a browser warning to Tor users when they visit the bogus website or were victims of MITM attacks.

“It was actually done pretty stupidly,” says Winter.

The National Security Agency wants to overwhelm Tor Anonymity

American Whistleblower Edward Snowden released a collection of classified NSA documents titled ‘Tor Stinks‘, which explain how the NSA agency has developed the capability to de-anonymize a small fraction of Tor users manually. Tor Stinks isn’t an architecture for surveillance on a large-scale, but it allows US agents to track specific individuals during their navigation inside the Tor network. *“We will never be able to de-anonymize all Tor users all the time, [but] with manual analysis we can de-anonymize a very small fraction of Tor users,”* reports of the slides disclosed.

In reality the intelligence agency is doing much more, trying to compromise the entire Tor network and degrading the user experience to dissuade people from using it.



TOP SECRET//COMINT// REL FVEY

Tor Stinks (U)

[redacted]

CT SIGDEV

[redacted]

JUN 2012

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20370101

TOP SECRET//COMINT// REL FVEY

Figure – NSA Tor Stinks Project to overwhelm Tor Anonymity

The NSA is operating in different ways to reach its goals. Its strategy relies on the following principles to unhinge Tor anonymity. It is running malicious Tor nodes to infiltrate the Tor networks, and at the same time, it is trying to exploit unknown flaws in every component of the anonymizing architecture, on both client and server sides.

Slides leaked by Snowden on the Stinks project reveal that the NSA is conducting the following operations:

- *Infiltrate Tor network running its Tor nodes*. Both the NSA and GCHQ run Tor nodes to track traffic back to a specific user. The method is based on the circuit reconstruction from the knowledge of the 'entry, relay and exit' nodes between the user and the destination website.
- Exploiting zero-day vulnerability of the Firefox browser bundled with Tor. With this technique, the NSA was able to get the user's IP address. In this way the FBI arrested the owner of the Freedom Hosting service provider accused of aiding and abetting child pornography.
- NSA also uses web cookies to track Tor users widely. The technique is effective also for the Tor Browser. The cookies are used to analyze the user's experience on the Internet. The intelligence agency owned or controlled a series of websites that was able to read last stored cookies from the browser on the victim's machine. With this technique, the agency collects the user's data, including the IP address. Of course. expert users can avoid this type of control in numerous ways, for example, using a dedicated browser for exclusive Tor navigation, using only the official preconfigured Tor bundle or

> properly managing the cookies stored on their machine. Unfortunately, the surveillance methods appeared effective for a huge quantity of individuals. I always suggest to use a virtual machine with a live OS for protecting your Tor anonymity. This way, cache and cookies will be lost once the machine is shut down. Documents leaked by Snowden show that the NSA is using online advertisements i.e. Google Ads to make their tracking sites popular on the Internet.

German public broadcaster ARD recently published a report on the use of the XKeyscore platform to compromise Tor anonymity. The media agency reported that two Germany-based Tor Directory Authority servers have been targeted by US intelligence. The broadcaster published for the first time the source code from Xkeyscore, even if ARD didn't provide information on its origin and how they received it.

XKeyscore gives the 'widest-reaching' collection of online data, analyzing the content of emails, social media and browsing history. In August 2014, The Guardian published an exclusive report on the NSA surveillance program, providing several NSA training slides from the secret program.

Facebook chats and private messages become accessible to the intelligence agents simply providing the Facebook user name and a date range for the investigation. XKeyscore in fact provides instruments necessary for the analysis that are conducted also without any legal authorization or a warrant.

"A top secret National Security Agency program allows analysts to search with no prior authorization through vast databases containing emails, online chats and the browsing histories of millions of individuals, according to documents provided by whistleblower Edward Snowden." The NSA boasts in training materials that the program, called XKeyscore, is its "widest-reaching" system for developing intelligence from the Internet.

The source code published by the ARD demonstrates that the NSA tracks people who are believed to live outside the US and who request Tor bridge information via e-mail or who search for or download Tor or the TAILS live operating system. The NSA was able to track their IP addresses. The XKeyScore analyzed by the experts includes IP addresses of the targeted Tor Directory Authority, part of the backbone of the Tor Network. These authorities are updated every hour with information related to new Tor relays.

The post also explains that the authors, including the popular expert Jacob Appelbaum, were targeted by the XKeyscore.

"Their research in this story is wholly independent from *the Tor Project and does not reflect the views of the Tor Project in any way … During the course of the investigation, it was further discovered that an additional computer system run by Jacob Appelbaum for his volunteer work with helping to run part of the Tor network was targeted by the NSA. Moreover, all members of this team are Tor users and appear to be have been targets of the mass surveillance described in the investigation,"* ARD stated.

Going deep in the source code, it is possible to verify that the NSA is also targeting users of anonymous remailer MixMinion.

```
[c]
/**
* Placeholder fingerprint for Tor hidden service addresses.
* Real fingerpritns will be fired by the plugins
* 'anonymizer/tor/plugin/onion/*'
*/
fingerprint('anonymizer/tor/hiddenservice/address') = nil;
// END_DEFINITION
// START_DEFINITION
appid('anonymizer/mailer/mixminion', 3.0,
viewer=$ascii_viewer) =
http_host('mixminion') or
ip('128.31.0.34');
// END_DEFINITION
[/c]
```

Law enforcement agencies, Tor Network and cybercrime

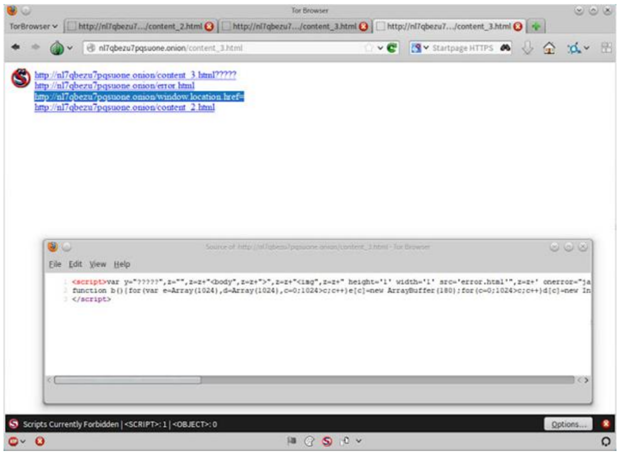
De-Anonymization of the Tor Network users is also a goal for law enforcement agencies that need to track users in order to identify and prevent illicit activities. The FBI last year revealed that experts at the Bureau had compromised the Freedom Hosting company during an investigation of child pornography. Freedom Hosting was probably the most popular Tor hidden service operator company. The FBI exploited a malicious script that takes advantage of a Firefox Zero-day to identify some users of the Tor anonymity network.

In an Irish court, the FBI Supervisory Special Agent Brooke Donahue revealed that the FBI had control of the Freedom Hosting company to investigate on child pornography activities. Freedom Hosting was considered by US law enforcement to be the largest child porn facilitator on the planet.

For its analysis, the FBI exploited a Firefox Zero-day (MFSA 2013-53) for Firefox 17, also confirmed by Mozilla, that allowed it to track Tor users. It exploited a flaw in the Tor browser to implant a tracking cookie which fingerprinted suspects through a specific external server.

"Security researcher Nils *reported that specially crafted web content using the* onreadystatechange *event and reloading of pages could sometimes cause a crash when unmapped memory is executed. This crash is potentially exploitable."*

The exploit is based on a JavaScript that is a tiny Windows executable hidden in a variable dubbed "Magneto". Magneto code looks up the victim's Windows hostname and MAC address and sends the information back to the FBI Virginia server, exposing the victim's real IP address. The script sends back the data with a standard HTTP web request outside the Tor Network.


Tor Browser
TorBrowser
http://nl7qbezu7.../content_2.html
http://nl7qbezu7.../content_3.html
http://nl7qbezu7.../content_3.html
nl7qbezu7pqsuone.onion/content_3.html
Startpage HTTPS
File
Edit
View
Help
Scripts Currently Forbidden | <SCRIPT>: 1 | <OBJECT>: 0
Options...

http://nl7qbezu7pqsuone.onion/content_3.html?????
http://nl7qbezu7pqsuone.onion/error.html
http://nl7qbezu7pqsuone.onion/window.location.href=
http://nl7qbezu7pqsuone.onion/content_2.html

```
<script>var y="?????",z="",z=z+"<body",z=z+">",z=z+"<img",z=z+" height='1' width='1' src='error.html'",z=z+' onerror="ja
function b(){for(var e=Array(1024),d=Array(1024),c=0;1024>c;c++)e[c]=new ArrayBuffer(180);for(c=0;1024>c;c++)d[c]=new In
</script>
```

Figure – Magneto script used by FBI

The investigation caused the identification and the arrest of Eric Eoin Marques, the 28-year-old Irishman owner and operator of Freedom Hosting.

Freedom Hosting hosted hundreds of websites, many of them used to conduct illegal activities taking advantage of the anonymity provided by the Tor network. Tor is ordinarily used by cybercriminals to conduct illicit activities like money laundering, exchanging of child porn material, renting for hacking services, and sale of drugs and weapons.

Freedom Hosting was offering hosting services to criminal gangs which were moving their business in the Deep Web. Consider that hundreds of hacking sites such as HackBB were hosted by the company.

Donahue revealed that the Freedom Hosting service hosted at least 100 child porn sites, providing illegal content to thousands of users, and claimed Marques had visited some of the sites himself.

Eric Eoin Marques knew he was being hunted, apparently he sent the earnings to his girlfriend over in Romania. The FBI, analyzing the Marques's seized computer, discovered that he had made inquiries about how to get a visa and entry into Russia, and residency and citizenship in the country.

Marques also made searches for a US passport template and a US passport hologram star. He probably was planning an escape.

Court documents and FBI files released under the FOIA have described the CIPAV (Computer and Internet Protocol Address Verifier) as software the FBI can deliver through a browser exploit to gather information from the suspect's machine and send it to on the server of the Bureau in Virginia.

The event is confirmation that the Tor network provides an extra layer of obfuscation, but it must be clear it does not provide bulletproof online anonymity. Many researchers demonstrated that it is possible to de-anonymize users by exploiting a flaw in the protocol itself, or in some of the numerous applications used, like web browser and live distro.

Break Tor network anonymity with just $3000

It is a common belief that to de-anonymize the Tor network, it is necessary to make a great effort in term of resources and computational capabilities. Many security experts have started to investigate the possibility that US intelligence and others have found a way to compromise the Tor network.

A few weeks ago, two hackers, Alexander Volynkin and Michael McCord, revealed to be able to de-anonymize Tor users easily. They also announced that they will present the results of their study at Black Hat 2014, despite that a few days ago they canceled their participation in the event.

"Unfortunately, Mr Volynkin will not be able to speak at the conference since the materials that he would be speaking about have not yet [been] approved by Carnegie Mellon University/Software Engineering Institute for public release," states the message posted on the official website of the event.

Christopher Soghoian, principal technologist with the American Civil Liberties Union, has speculated that the researchers might have feared to be sued by criminal prosecution for illegal monitoring of Tor exit traffic.

"Monitoring Tor exit traffic is potentially a violation of several federal criminal statutes," he added.

The expert was preparing a presentation, YOU DON'T HAVE TO BE THE NSA TO BREAK TOR: DEANONYMIZING USERS ON A BUDGET, to explain how to identify Tor users with a very small budget, just $3,000.

"There is nothing that prevents you from using your resources to de-anonymize the network's users instead by exploiting fundamental flaws in Tor design and implementation. And you don't need the NSA budget to do so. Looking for the IP address of a Tor user? Not a problem. Trying to uncover the location of a Hidden Service? Done. We know because we tested it, in the wild ... In this talk, we demonstrate how the distributed nature, combined with newly discovered shortcomings in design and implementation of the Tor network, can be abused to break Tor anonymity," are the statements used by the two researchers to describe their work.

According to the researchers, it is possible to de-anonymize users with a limited budget. The worrying news is that a persistent adversary like an intelligence agency *"with a handful of powerful servers and a couple gigabit links can de-anonymize hundreds of thousands of Tor clients and thousands of hidden services within a couple of months."*

The discovery made by the researchers, even if it was never publicly disclosed, seems to confirm the fact that the popular anonymizing network is affected by serious flaws that could be exploited by attackers to track users.

One of the creators of the Tor project, Roger Dingledine, speaking of the discovery announced by the two researchers, admitted that the Tor Project had been "informally" shown some of the materials that would have been presented by the two researchers.

"In response to our questions, we were informally shown some materials. We never received slides or any description of what would be presented in the talk itself beyond what was available on the BlackHat *Webpage.*

"I think I have a handle on what they did, and how to fix it. We've been trying to find delicate ways to explain that we think we know what they did, but also it sure would have been smoother if they'd opted to tell us everything. The main reason for trying to be delicate is that I don't want to discourage future researchers from telling us about neat things that they find. I'm currently waiting for them to answer their mail so I can proceed … Based on our current plans, we'll be putting out a fix that relays can apply that should close the particular bug they found. The bug is a nice bug, but it isn't the end of the world," he added.

The Dingledine' words confirm that there is a flaw in the Tor architecture that the two scientists probably exploited. This means that the software may have been already compromised in the past by Intelligence agencies.

Ongoing attacks

As we discussed in the previous paragraph, law enforcement, intelligence agencies and individuals are interested in de-anonymizing Tor users for various purposes. Now it's time to analyze a real ongoing attack, explaining the modus operandi of attackers.

On July 30th, the members of the Tor project published on the official website a security advisory to reveal that earlier in the month, on July 4th, 2014, a group of relays was targeted by a cyber attack conducted with the goal to de-anonymize users. The experts on the Tor Project noticed that bad actors were targeting relays to track users accessing Tor networks or access Tor hidden services.

"They appear to have been targeting people who operate or access Tor hidden services. The attack involved modifying Tor protocol headers to do traffic confirmation attacks.

"The particular confirmation attack they used was an active attack where the relay on one end injects a signal into the Tor protocol headers, and then the relay on the other end reads the signal. These attacking relays were stable enough to get the HSDir ("suitable for hidden service directory") and Guard ("suitable for being an entry guard") consensus flags. Then they injected the signal whenever they were used as a hidden service directory, and looked for an injected signal whenever they were used as an entry guard.

The technique is simple as efficient. The attack is possible when the attacker controls or observes the relays on both ends of a Tor circuit and then compares traffic timing, volume, or other characteristics to conclude that the two relays are part of the same circuit, which routes information from source to destination.

In the case of the first relay in the circuit ("entry guard"), it knows the IP address of the user, and the last relay in the circuit ("exit nodes") knows the resource or destination the user is accessing. Then the attacker is able to de-anonymize Tor users.

Attackers were leveraging a critical flaw in Tor architecture to modify protocol headers in order to perform a traffic confirmation attack and inject a special code into the protocol header used by attackers to compare certain metrics from relays to de-anonymize users.

115 malicious fast non-exit relays (6.4% of the whole Tor network) were involved in the attack. The servers were actively monitoring the relays on both ends of a Tor circuit in an effort to de-anonymize users. The malicious relays were running Tor version 50.7.0.0/16 or 204.45.0.0/16 and bad actors were using them trying to de-anonymize Tor users who visit and run so-called hidden services. The malicious relays joined the Tor network on January 30th, 2014 and experts at Tor Project removed them from the network on July 4th, 2014.

The members of the Tor project team also advised hidden service operators to change the location of their hidden service.

"While we don't know when they started doing the attack, users who operated or accessed hidden services from early February through July 4 should assume they were affected," Tor said.

When users access the Tor network with Tor software, their IP address is not visible and it appears to the Internet as the IP address of a Tor exit relay, which can be anywhere.

Bad actors who were running the confirmation attack were looking for users who fetched hidden service descriptors. This means that attackers were not able to see pages loaded by users, nor whether users visited the hidden service they looked up.

"The attack probably also tried to learn who published hidden service descriptors, which would allow the attackers to learn the location of that hidden service. In theory the attack could also be used to link users to their destinations on normal Tor circuits too, but we found no evidence that the attackers operated any exit relays, making this attack less likely. And finally, we don't know how much data the attackers kept, and due to the way the attack was deployed (more details below), their protocol header modifications might have aided other attackers in de-anonymizing *users too,"* states the security advisory.

In order to close the critical flaw, the Tor Project Team is suggesting Tor Relay Operators to upgrade Tor software to a recent release, either 0.2.4.23 or 0.2.5.6-alpha. Tor Project released a software update to prevent such attacks.

Conclusions

Law enforcement agencies and Intelligence are spending a great effort to de-anonymize the user experience on the Tor network, to discourage the use of anonymizing networks.

Attackers can follow two directions:

- Try to break encryption used to anonymize the traffic.
- Try to exploit flaws in one of the numerous components present in the anonymizing architecture.

As demonstrated by recent attacks on anonymizing software like Tails Live Distribution, probably the second choice is the most suitable. The presence of an unknown flaw in one of these components could allow a compromise of the entire architecture.

Attackers know this, and they are concentrating all their effort to discover such flaws … but if you are a researcher, do not forget that every day anonymizing networks allow many individuals to avoid censorship and monitoring operated by authoritarian regimes.

References

http://securityaffairs.co/wordpress/26395/hacking/tor-network-broken.html

http://securityaffairs.co/wordpress/26982/hacking/tor-working-fix-flaw.html

http://securityaffairs.co/wordpress/27019/hacking/russian-government-crack-tor.html

http://www.theregister.co.uk/2014/07/25/putin_crack_tor_for_me_and_ill_make_you_a_millionaire/

http://securityaffairs.co/wordpress/27193/hacking/attacks-against-tor-network.html

http://securityaffairs.co/wordpress/5650/cyber-crime/what-is-the-deep-web-a-first-trip-into-the-abyss.html

https://blog.torproject.org/blog/tor-security-advisory-relay-early-traffic-confirmation-attack http://www.cs.kau.se/philwint/spoiled_onions/techreport.pdf

http://securityaffairs.co/wordpress/18397/hacking/tor-anonymity-tor-stinks.html

http://www.bbc.com/news/technology-28573625

http://www.wired.com/2013/09/freedom-hosting-fbi/all/1

http://securityaffairs.co/wordpress/21535/cyber-crime/russia-spying-tor-network-exit-nodes.html

http://securityaffairs.co/wordpress/26335/intelligence/xkeyscore-hit-tor-authority-server.html

nd Online Anonymity”

ke NSA and Russian Intelligence are able to exploit flaws in onymizing architecture thereby de-anonymize the user. The d.

are marked *

https://blog.torproject.org/blog/one-cell-enough

Email *

Posted: August 6, 2014

Share:

Website

Po

Author

Pierluigi Paganini

VIEW PROFILE

d Articles

Pierluigi is member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group, member of Cyber G7 Workgroup of the Italian Ministry of Foreign Affairs and International Cooperation, Professor and Director of the Master in Cyber Security at the Link Campus University. He is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines.

communications via Unisoc baseband vulnerability

Author Image August 4, 2022 **Pedro Tavares**

detector

Author Image May 17, 2022 **Pedro Tavares**

Hacking

Top tools for password-spraying attacks in active directory networks

Author Image January 25, 2022 **Pedro Tavares**

Hacking

NPK: Free tool to crack password hashes with AWS

Author Image December 16, 2021 **Lester Obbayi**

Topics

- Hacking
- Penetration testing
- Cyber ranges
- Capture the flag
- Malware analysis
- Professional development
- General security
- News
- Security awareness
- Phishing
- Management, compliance & auditing
- Digital forensics
- Threat intelligence
- DoD 8570
- *View all topics*

Certifications

- CISSP
- CCSP
- CGEIT
- CEH
- CCNA
- CISA
- CISM
- CRISC
- A+
- Network+
- Security+
- CASP+
- PMP
- CySA+
- CMMC
- Microsoft Azure
- *View all certifications*

Careers

- IT auditor
- Cybersecurity architect
- Cybercrime investigator
- Penetration tester
- Cybersecurity consultant
- Cybersecurity analyst
- Cybersecurity engineer
- Cybersecurity manager
- Incident responder
- Information security auditor
- Information security manager
- *View all careers*

Company

- Contact us
- About Infosec
- Work at Infosec
- Newsroom
- Partner program