Defending Against Malicious Cyber Activity Originating from Tor

This advisory—written by the Cybersecurity Security and Infrastructure Security Agency (CISA) with contributions from the Federal Bureau of Investigation (FBI)—highlights risks associated with Tor, along with technical details and recommendations for mitigation. Cyber threat actors can use Tor software and network infrastructure for anonymity and obfuscation purposes to clandestinely conduct malicious cyber operations.[1,2,3]

Tor (aka The Onion Router) is software that allows users to browse the web anonymously by encrypting and routing requests through multiple relay layers or nodes. This software is maintained by the Tor Project, a nonprofit organization that provides internet anonymity and anti-censorship tools. While Tor can be used to promote democracy and free, anonymous use of the internet, it also provides an avenue for malicious actors to conceal their activity because identity and point of origin cannot be determined for a Tor software user. Using the Onion Routing Protocol, Tor software obfuscates a user's identity from anyone seeking to monitor online activity (e.g., nation states, surveillance organizations, information security tools). This is possible because the online activity of someone using Tor software appears to originate from the Internet Protocol (IP) address of a Tor exit node, as opposed to the IP address of the user's computer.

CISA and the FBI recommend that organizations assess their individual risk of compromise via Tor and take appropriate mitigations to block or closely monitor inbound and outbound traffic from known Tor nodes.

---

[1] CISA Alert published April 2020: *Continued Threat Actor Exploitation Post Pulse Secure VPN Patching*. Cyber threat actors used Connection Proxies—such as Tor infrastructure and virtual private servers (VPSs)—to minimize the chance of detection when they connected to victim VPN appliances.

[2] CISA Advisory published February 2017: *Enhanced Analysis of GRIZZLY STEPPE Activity*. GRIZZLY STEPPE actors have infected pirated software in torrent services and leveraged TOR exit nodes to deliver to malware since at least 2014.

[3] FBI Press release published November 2014: *More Than 400 .Onion Addresses, Including Dozens of 'Dark Market' Sites, Targeted as Part of Global Enforcement Action on Tor Network*. Advertised goods and services included: computer-hacking tools and services.

RISK EVALUATION

Malicious cyber actors use Tor to mask their identity when engaging in malicious cyber activity impacting the confidentiality, integrity, and availability of an organization's information systems and data. Examples of this activity include performing reconnaissance, penetrating systems, exfiltrating and manipulating data, and taking services offline through denial-of-service attacks and delivery of ransomware payloads. Threat actors have relayed their command and control (C2) server communications—used to control systems infected with malware—through Tor, obscuring the identity (location and ownership) of those servers.

The use of Tor in this context allows threat actors to remain anonymous, making it difficult for network defenders and authorities to perform system recovery and respond to cyberattacks. Organizations that do not take steps to block or monitor Tor traffic are at heightened risk of being targeted and exploited by threat actors hiding their identity and intentions using Tor.

The risk of being the target of malicious activity routed through Tor is unique to each organization. An organization should determine its individual risk by assessing the likelihood that a threat actor will target its systems or data and the probability of the threat actor's success given current mitigations and controls. This assessment should consider legitimate reasons that non-malicious users may prefer to, or need to, use Tor for accessing the network. Organizations should evaluate their mitigation decisions against threats to their organization from advanced persistent threats (APTs), moderately sophisticated attackers, and low-skilled individual hackers, all of whom have leveraged Tor to carry out reconnaissance and attacks in the past.

TECHNICAL DETAILS

Tor obfuscates the source and destination of a web request. This allows users to conceal information about their activities on the web—such as their location and network usage—from the recipients of that traffic, as well as third parties who may conduct network surveillance or traffic analysis. Tor encrypts a user's traffic and routes the traffic through at least three Tor nodes, or relays, so that the user's starting IP address and request is masked from network and traffic observers during transit. Once the request reaches its intended destination, it exits Tor through a public Tor exit node. Anyone conducting monitoring or analysis will only see the traffic coming from the Tor exit node and will not be able to determine the original IP address of the request.

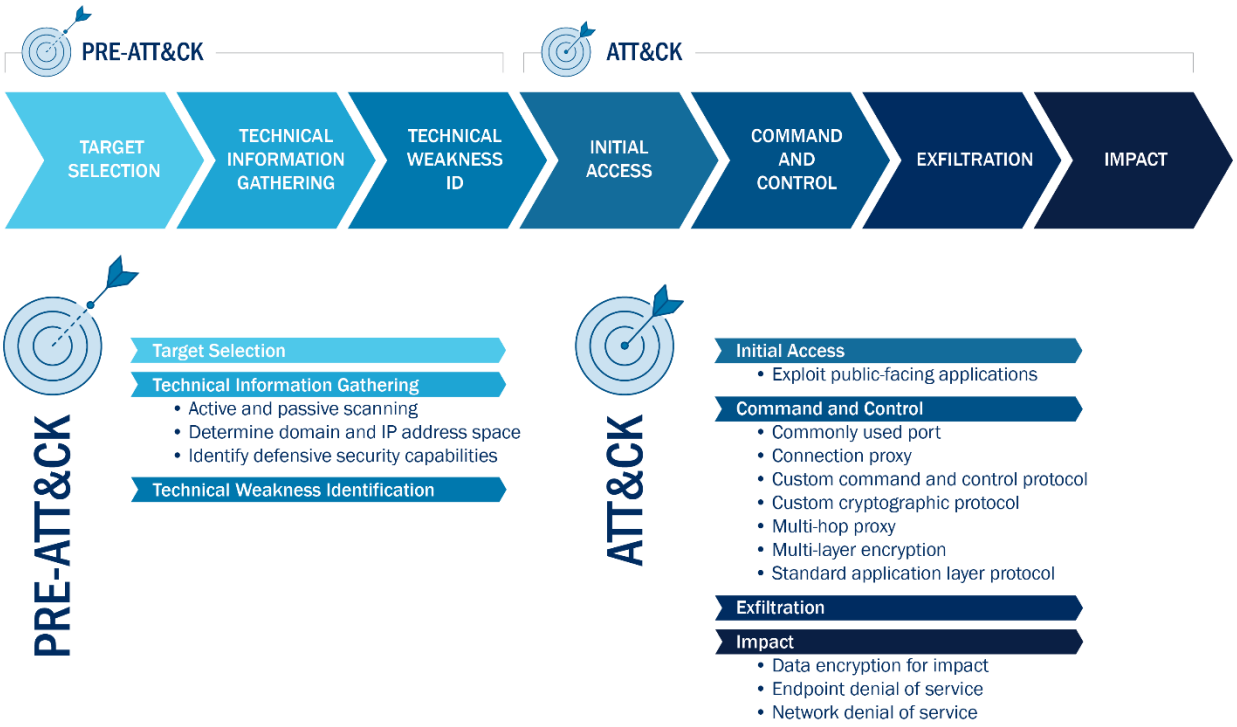

*Figure 1: Malicious tactics and techniques aided by Tor, mapped to the **MITRE ATT&CK framework***

Malicious Tactics and Techniques Aided by Tor

This advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) and Pre-ATT&CK framework. See the ATT&CK for Enterprise and Pre-ATT&CK frameworks for referenced threat actor techniques.

Threat actors use Tor to create a layer of anonymity to conceal malicious activity at different stages of network compromise. Their tactics and techniques—illustrated in figure 1 above—include:

Pre-ATT&CK

- *Target Selection* [TA0014]
- *Technical Information Gathering* [TA0015]
    - *Conduct Active Scanning* [T1254]
    - *Conduct Passive Scanning* [T1253]
    - *Determine domain and IP address space* [T1250]
    - *Identify security defensive capabilities* [T1263]
- *Technical Weakness Identification* [TA0018]

ATT&CK

- *Initial Access* [TA0001]
    - *Exploit Public-Facing Applications* [T1190]

- *Command and Control* [TA0011]
  - *Commonly Used Port* [T1043]
  - *Connection Proxy* [T1090]
  - *Custom Command and Control Protocol* [T1094]
  - *Custom Cryptographic Protocol* [T1024]
  - *Multi-hop Proxy* [T1188]
  - *Multilayer Encryption* [T1079]
  - *Standard Application Layer Protocol* [T1071]
- *Exfiltration* [TA0010]
- *Impact* [TA0040]
  - *Data Encrypted for Impact* [T1486]
  - *Endpoint Denial of Service* [T1499]
  - *Network Denial of Service* [T1498]

Key Indicators of Malicious Activity via Tor

While Tor obfuscates a user from being identified through standard security tools, network defenders can leverage various network, endpoint, and security appliance logs to detect the use of Tor, including potentially malicious activity involving Tor, through indicator- or behavior-based analysis.

Using an indicator-based approach, network defenders can leverage security information and event management (SIEM) tools and other log analysis platforms to flag suspicious activities involving the IP addresses of Tor exit nodes. The list of Tor exit node IP addresses is actively maintained by the Tor Project's Exit List Service, which offers both real-time query and bulk download interfaces (see https://blog.torproject.org/changes-tor-exit-list-service). Organizations preferring bulk download may consider automated data ingest solutions, given the highly dynamic nature of the Tor exit list, which is updated hourly. Network defenders should closely inspect evidence of substantial transactions with Tor exit nodes—revealed in netflow, packet capture (PCAP), and web server logs—to infer the context of the activity and to discern any malicious behavior that could represent reconnaissance, exploitation, C2, or data exfiltration.

Using a behavior-based approach, network defenders can uncover suspicious Tor activity by searching for the operational patterns of Tor client software and protocols. Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports commonly affiliated with Tor include 9001, 9030, 9040, 9050, 9051, and 9150. Highly structured Domain Name Service (DNS) queries for domain names ending with the suffix torproject.org is another behavior exhibited by hosts running Tor software. In addition, DNS queries for domains ending in .onion is a behavior exhibited by misconfigured Tor clients, which may be attempting to beacon to malicious Tor hidden services.

Organizations should research and enable the pre-existing Tor detection and mitigation capabilities within their existing endpoint and network security solutions, as these often employ effective detection logic. Solutions such as web application firewalls, router firewalls, and host/network intrusion detection systems may already provide some level of Tor detection capability.

MITIGATIONS

Organizations can implement mitigations of varying complexity and restrictiveness to reduce the risk posed by threat actors who use Tor to carry out malicious activities. However, mitigation actions can also impact the access of legitimate users who leverage Tor to protect their privacy when visiting an organization's internet-facing assets. Organizations should evaluate their probable risk, available resources, and impact to legitimate, non-malicious, Tor users before applying mitigation actions.

- **Most restrictive approach: Block all web traffic to and from public Tor entry and exit nodes.** Organizations that wish to take a conservative or less resource-intensive approach to reduce the risk posed by threat actors' use of Tor should implement tools that restrict all traffic—malicious and legitimate—to and from Tor entry and exit nodes. Of note, blocking known Tor nodes does not completely eliminate the threat of malicious actors using Tor for anonymity, as additional Tor network access points, or bridges, are not all listed publicly. See table 1 for the most restrictive mitigation practices.

Table 1: Most restrictive mitigation practices

Type	Level of Effort	Technical Implementation	Impact
Baseline Activity	Low/Medium	Require organization to maintain up-to-date lists of known Tor exit and entry node IP addresses. Public lists are available on the internet, but frequency of updates and accuracy varies depending on the source. The Tor Project maintains an authoritative list.	Up-to-date awareness of known Tor nodes to enable blocking
External Policies	Medium	Set external policies to block incoming traffic from known Tor exit nodes to prevent malicious reconnaissance and exploit attempts. Network security tools (e.g., next-generation firewalls, proxies) may have configuration settings to apply these policies.	Block inbound network traffic, both malicious and legitimate, from reaching the organization's domain from known Tor exit nodes
Internal Policies	Medium	Set internal policies to block outgoing traffic to Tor entry nodes to prevent data exfiltration and C2 traffic. Network security tools (e.g., next-generation firewalls, proxies) may have configuration settings to apply these policies.	Block outbound network traffic, both malicious and legitimate, from leaving the organization's domain into known Tor entry nodes

- **Less restrictive approach: Tailor monitoring, analysis, and blocking of web traffic to and from public Tor entry and exit nodes**. There are instances in which legitimate users may leverage Tor for internet browsing and other non-malicious purposes. For example, deployed military or other overseas voters may use Tor as part of the voting process to escape monitoring by foreign governments. Such users may use Tor when visiting elections-related websites, to check voter registration status, or to mark and then cast absentee ballots via email or web portal. Similarly, some users may use Tor to avoid tracking by advertisers when browsing the internet. Organizations that do not wish to block legitimate traffic to/from Tor entry/exit nodes should consider adopting practices that allow for network monitoring and traffic analysis for traffic from those nodes, and then consider appropriate blocking. This approach can be resource intensive but will allow greater flexibility and adaptation of defensive

Table 2: Less restrictive mitigation practices

Type	Level of Effort	Technical Implementation	Impact
Known Tor Nodes	Low/Medium	Require the organization to maintain up-to-date lists of known Tor exit and entry node IP addresses. The Tor Project maintains an authoritative list.	Up-to-date awareness of known Tor nodes to enable baselining/allow blocking
SIEM Correlation	Low/Medium	Integrate network security and SIEM tools that correlate logs.	Enhanced understanding of legitimate/expected Tor use for inbound/outbound traffic
Baseline	Medium	Analyze traffic to determine normal patterns of behavior; legitimate vs. anomalous uses of Tor. Baseline existing Tor traffic to/from known entry/exit nodes over a period of months. Inspect traffic to understand legitimate traffic; level-set the organization's risk tolerance for blocking or allowing Tor traffic to/from specific services.	Baseline understanding of legitimate vs. potentially anomalous Tor uses

Internal / External Policies	Medium/High	Institute behavioral signatures/rules to block unexpected/potentially malicious activity and allow legitimate activity. Examine activity between any ephemeral port and Tor IP—this could be malicious data exfiltration or C2 traffic (except where use of outbound Tor entry nodes is expected). Monitor for use of TCP/UDP ports 9001, 9030, 9040, 9050, 9051, 9150, and TCP ports 443* and 8443. Monitor and/or block inbound connections from Tor exit nodes to IP addresses and ports for which external connections are not expected (i.e., other than VPN gateways, mail ports, web ports). Associated ports are applicable for client -> guard/relay traffic monitoring and analysis but not monitoring for exit node -> a network destination. Monitor and examine any large dataflows between networks and Tor IP addresses, regardless of port, as this could be unauthorized data exfiltration. **Since port 443 is the most common port for secure web traffic, generically monitoring 443 may produce a high volume of false positives; network traffic tools can be used to assist in this analysis.*	Legitimate traffic via Tor entry/exit nodes is permitted and unexpected/potentially malicious activity via Tor entry/exit nodes is blocked

- **Blended approach: Block all Tor traffic to some resources, allow and monitor for others.** Given the various licit and illicit uses of Tor, a blended approach may be an appropriate risk mitigation strategy for some organizations (i.e., intentionally allowing traffic to/from Tor only for specific websites and services where legitimate use may be expected and blocking all Tor traffic to/from non-excepted processes/services). This may require continuous re-evaluation as an entity considers its own risk tolerance associated with different applications. The level of effort to implement this approach is high.

Considerations for Blocking Use of Tor

Sophisticated threat actors may leverage additional anonymization technologies—such as virtual private networks (VPNs)—and configurable features within Tor—such as Tor bridges and pluggable transports—to circumvent detection and blocking. Blocking the use of known Tor nodes may not effectively mitigate all hazards but may protect against less sophisticated actors. For example, blocking outbound traffic to known Tor entry nodes could have an appreciable impact in blocking less sophisticated malware from successfully beaconing out to hidden C2 machines obfuscated by Tor. Ultimately, each entity must consider its own internal thresholds and risk tolerance when determining a risk mitigation approach associated with Tor.