EUROPOL
EC3 | European Cybercrime Centre

The Hague, April 2017

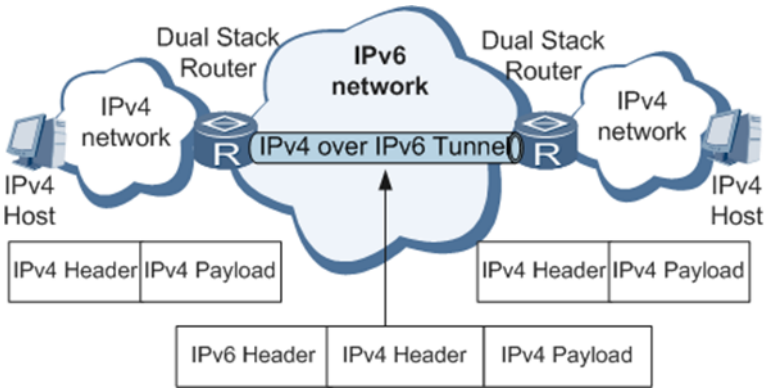
Intelligence Notification No. 7/2017

CYBER BITS
Series: Trend

IPv6 Vulnerability

What happened?

Bernhards Blumbergs, Mauno Pihelgas, Markus Kont, Olaf Maennel and Risto Vaarandi have released a report detailing the security holes that exist as a result of IPv4 to IPv6 transition tools. With great technical complexity, it details how the mechanisms of IPv6 transition could allow the set-up of egress communication channels over an IPv4-only or dual-stack network while evading detection by a Network Intrusion Detection System (NIDS).



mage retrieve from: http://support.huawei.com/enterprise/docinforeader.action?contentId=DOC1000097281&partNo=10152

The research, carried out jointly by the NATO Cooperative Cyber Defence Centre of Excellence and the Tallinn University of Technology shows that current NIDS solutions have serious drawbacks for handling IPv6 traffic. Addressing these shortcomings would require a redevelopment of the NIDS reassembly packet streams principles, and correlation of distinct sessions.

It was already known that a proof-of-concept tool for the establishment of Covert channels over ICMPv6 has demonstrated the potential for such an approach, though it has not been released publicly. Techniques for evading NIDS based on mobile IPv6 implementations reveal that it is possible to trick NIDS using Dynamically-Changing Communication Channels. Also, it may be viable to create a covert channel by hiding information within IPv6 and its extension headers. NIDS systems and firewall evasions based on IPv6 packet fragmentation and extension header chaining attacks have been acknowledged.

The Internet Protocol Version 6 (IPv6) transition opens a wide scope for potential attack vectors. Tunnel-based IPv6 transition mechanisms could allow the set-up of egress communication channels over an IPv4-only or dual-stack network while evading detection by a network intrusion detection system (NIDS).

Increased usage of IPv6 in attacks results in long-term persistence, sensitive information exfiltration, or system remote control. Effective tools are required for the execution of security operations for assessment of possible attack vectors related to IPv6 security.

Being more exact the protocol tunnelling and IPv6 tunnelling-based transition mechanisms pose a major security risk, as they allow bypassing of improperly-configured or IPv4-only network security devices. Moreover, dual-stack hosts and Internet browsers favour IPv6 over IPv4, which in some cases raises security concerns as this may not be anticipated by network security personnel. Various protocol tunnelling approaches can be used to set up a covert channel by encapsulating exfiltrated information in networking protocols, such as DNS, HTTP(S), SSH, ICMP, RTP, FTP, SSH over HTTP, and peer-to-peer.

How does it work?

The research has implemented the following covert channel techniques: protocol tunnelling, a proof-of-concept nc64 tool and a proof-of-concept tun64 tool. These proof-of-concept tools are written in Python version 3 using standard libraries.

The researchers evaluated commonly used exfiltration tools in an automated and virtualized environment, and assessed covert channel detection methods in the context of insider threat.

In most cases, the nc64 tool avoided being detected, and shows which protocol/port combinations can be used to minimize detection by selected NIDS solutions. In comparison with other exfiltration tools, nc64 performed very well on avoiding rule-based detection, and moreover could potentially elude payload inspection.

In contrast, the tun64 tool was detected in the majority of cases, since protocol-41 and protocol-47 triggered the rules and generated warning messages by NIDSs. IPv6 to IPv4 tunnelling emulation was detected when TCP or IPv6inIPv4-in-GRE encapsulation was used, suggesting that double encapsulation is considered more suspicious. However, if an organization relies on IPv6 tunnelling-based transition mechanisms utilizing IPv6inIPv4 or GRE encapsulation, such warnings might be silenced or ignored by network-monitoring personnel. In contrast to other tunnelling tools, the approach taken by tun64 is feasible only if the network conditions comply with the specific operational requirements.

Why do you need to know?

- Both Law Enforcement and private entities should make themselves aware of the possible risks involved in IPv6 vulnerabilities. By exploiting this vulnerabilities it is possible to set up undetectable communications channels across networks that could be used to pull out data and control systems remotely.
- According to relevant transition technologies, the research describes two newly-developed IPv6 transition mechanism-based proof-of-concept tools for the establishment of covert information exfiltration channels, and compare their performance against common tunnelling mechanisms.
- An analysis of the generated test cases confirms that IPv6 and various evasion techniques pose a difficult task for network security monitoring. While detection of various transition mechanisms is relatively straightforward, other evasion methods prove more challenging. Additionally, some solutions do not yet fully support IPv6.

Source: https://ccdcoe.org/sites/default/files/multimedia/pdf/ip6eva_0.pdf

EC3 would welcome feedback on this note. Please mail to O31@europol.europa.eu.
(note that "O" is *a letter not a number)*