DNS tunnel traffic detected (DNS_Tunnel_Detected)

About this signature or vulnerability

Proventia Server IPS for Linux technology, Proventia Network IPS, IBM Security Host Protection for Desktops, RealSecure Server Sensor, RealSecure Network, Proventia Network IDS, Proventia Network MFS, Proventia-G 1.1 and earlier, IBM Security Host Protection for Servers (Windows), Virtual Server Protection for Vmware, IBM Security Host Protection for Servers (Unix):

This signature detects a DNS tunnel characterized by repeated subdomain queries and answers for a common domain using a specific DNS TXT record format. The authoritative server for the common domain would be a specially configured DNS server designed to host DNS tunnel sessions. The tunnel detection is based upon seeing a large number of DNS transactions (pam.dns.tunnel.detection.total) having a minimum payload (pam.dns.tunnel.min.data.length) between the same two IP addresses. To count transactions towards DNS tunnel detection, a transaction rate (pam.dns.tunnel.detection.rate) must be met or exceeded each second until DNS_Tunnel_Detected triggers. Thereafter, the traffic is monitored until an idle timeout occurs (pam.dns.tunnel.idle.timeout), and signature re-reporting is limited to once every pam.dns.tunnel.report.interval seconds.

DNSBL (DNS-based Blacklist) and DNSWL (DNS-based Whitelist) servers provide information about IP addresses, often in regards to spamming, using RFC 5782 (or a similar format) that includes the use of DNS TXT records for information exchange. When using TXT records, these services are essentially DNS tunnels. To avoid triggering on DNSBL and DNSWL services, the following domains have been whitelisted and will not trigger DNS_Tunnel_Detected:

abuseat.org, ahbl.org, atlbl.net, baracudacentral.org, blocklist.de, datapacket.net, dnswl.org, drand.net, dronebl.org, fabel.dk, gbudb.net, hostkarma.com, inps.de, ipquery.org, junkemailfilter.com, manitu.net, njabl.org, orbitrbl.com, proofpoint.com, proxybl.org, rfc-ignorant.org, sorbs.net, spamcannibal.org, spamcop.net, spameatingmonkey.com, spamhaus.org, spamrats.com, surbl.org, surriel.com, tiopan.com, trendmicro.com, uceprotect.net, unsubscore.com, v4bl.org, wpbl.info

This signature detects a DNS tunnel characterized by repeated subdomain queries and answers for a common domain using a specific DNS record format. The authoritative server for the common domain would be a specially configured DNS server designed to host DNS tunnel sessions. The tunnel detection is based upon seeing a large number of DNS transactions (pam.dns.tunnel.detection.total) having a minimum payload (pam.dns.tunnel.min.data.length) between the same two IP addresses. To count transactions towards DNS tunnel detection, a transaction rate (pam.dns.tunnel.detection.rate) must be met or exceeded each second until DNS_Tunnel_Detected triggers. Thereafter, the traffic is monitored until an idle timeout occurs (pam.dns.tunnel.idle.timeout), and signature re-reporting is limited to once every pam.dns.tunnel.report.interval seconds.

Default risk level

Low

Sensors that have this signature

Proventia Server IPS for Linux technology: 30.110, Proventia Network IPS: XPU 30.110, IBM Security Host Protection for Desktops: 2580, RealSecure Server Sensor: XPU 30.110, RealSecure Network: XPU 30.110, Proventia Network IDS: XPU 30.110, Proventia Network MFS: XPU 30.110, Proventia-G 1.1 and earlier: XPU 30.110, IBM Security Host Protection for Servers (Windows): 2.1.14.2580, Virtual Server Protection for Vmware: XPU 30.110, IBM Security Host Protection for Servers (Unix): 2.2.2

Systems affected

DNS DNS

Type

Suspicious Activity

Vulnerability description

A DNS Tunnel allows passing arbitrary user data through most networks to and from a specially configured DNS server. The user data is encrypted and hidden within DNS requests and responses associated with a domain owned by the specially configured DNS server. The DNS traffic can pass freely through most networks and the Internet via the DNS protocol, circumventing firewalls and network policies.

How to remove this vulnerability

This event is for informational purposes only.

References

ISS X-Force
DNS tunnel traffic detected
http://www.iss.net/security_center/static/62621.php