Corelight Collections

Encrypted Traffic and C2 Collection Detections and Inferences

The Encrypted Traffic Collection

Packages

Package	Description
Cert Hygiene	This package tracks risk indicators in your TLS traffic, such as newly minted certificates, expiring certificates, and the use of weak encryption keys.
Encrypted DNS Server Detection	This package detects DNS-over-HTTPS traffic.
Encryption Detection	This package tracks & logs information about visibility of transport flows.
RDP Inference	This package provides information about encrypted TLS connections through client, authentication, and behavioral inferences
SSH Inference	This package makes inferences about the purpose of SSH connections, such as keystrokes or file transfers, and attempted exploits.
SSH Stepping Stones	This package detects a series of intermediary hosts connected via SSH.

Notices

- RDP::Password_Guessing
- RDP::Login_By_Password_Guesser
- RDP::Joined_A_Lot_Of_Channels
- SSH::Authentication_Bypass
- SSH::Interactive_Keystrokes
- SSH::Bruteforce_Auth_Success
- SSH::Tunnel_Prototcol
- SSH::No_Remote_Command
- SSH::Agent_Forwarding_Requested
- SSL::Certificate_Expired
- SSL::Certificate_Expires_Soon
- SSL::Certificate_Not_ Valid_Yet
- SSL::Certificate_Is_New
- SSL::Invalid_Server_Cert
- SSL::Weak_Key
- SSL::Old_Version
- SSL::Weak_Cipher
- Viz::UnencryptedService
- Viz::CustomCrypto

RDP Inferences

Inference code	Inference Name	Description
FC	FreeRDP Driven Client	Indicates a CLI tool client (likely FreeRDP-based).
MSC	Metasploit Scanner Client	Indicates a Metasploit client.
HBC	THC-Hydra Bruteforce Client	Indicates a Hydra client.
CBC	Crowbar Bruteforce Client	Indicates a Crowbar client.
SLC	SharpRDP Lateral Movement Client	Indicates a SharpRDP client.
SOC	Scanner Other Client	Indicates that the client is likely a scanner or exploit tool that the package can't specifically identify (for example, rdpscan or impacket).
RCGA	Remote Credential Guard Authentication	Indicates that the client authenticated using Restricted Admin Mode.

RAMA	Restricted Admin Mode Authentication	Indicates a Metasploit client.
APWA	Automated NTLM Password Authentication	Indicates that the client authenticated using an NTLM password that was provided before the connection was initiated.
IPWA	Interactive NTLM Password Authentication	Indicates that the client authenticated using an NTLM password that was provided after the connection was initiated, suggesting a human- driven connection.
SLC	SharpRDP Lateral Movement Client	Indicates a SharpRDP client.
SOC	Scanner Other Client	Indicates that the client is likely a scanner or exploit tool that the package can't specifically identify (for example, rdpscan or impacket).
SLH	SLH Slow Handshake	Indicates that the handshake (RDPBCGR connection sequence) took an unusually long time to complete.

SSH Inferences

Inference code	Inference Name	Description
ABP	Client Authentication Bypass	A client wasn't adhering to expectations of SSH either through server exploit or by the client and server switching to a protocol other than SSH after encryption begins.
BF	Client Brute Force Guessing	A client made a number of authentication attempts that exceeded some configured, per-connection threshold.
BFS	Client Brute Force Success	A client made a number of authentication attempts that exceeded some configured, per-connection threshold.
SFD	Small Client File Download	A file transfer occurred in which the server sent a sequence of bytes to the client.
LFD	Large Client File Download	A file transfer occurred in which the server sent a sequence of bytes to the client. Large files are identified dynamically based on trains of MTU-sized packets.

SFU	Small Client File Upload	A file transfer occurred in which the client sent a sequence of bytes to the server.
LFU	Large Client File Upload	A file transfer occurred in which the client sent a sequence of bytes to the server.
KS	Keystrokes	An interactive session occurred in which the client set user-driven keystrokes to the server.
SC	Capabilities Scanning	A client exchanged capabilities with the server and then disconnected.
SP	Other Scanning	A client and server didn't exchange encrypted packets; client wasn't a version or capabilities scanner.
SV	Version Scanning	A client exchanged version strings with the server and then disconnected.
SA	Authentication Scanning	The client scanned authentication methods with the server and then disconnected.
APWA	Automated Password Auth	The client authenticated with an automated password tool (like sshpass).
IPWA	Interactive Password Auth	The client typed their password to authenticate.
PKA	Public Key Authentication	The client automatically authenticated using pubkey authentication.
NA	None Authentication	The client successfully authenticated using the None method.
MFA	Multifactor authentication	The server required second form of authentication (a code) after password or public key was accepted, and client provided it.
UA	Unknown authentication	The authentication method is not determined or is unknown.
AUTO	Automated interaction	The client is a script or automated utility and not driven by a user.
BAN	Server Banner	The server sent the client a pre-authentication banner, likely for legal reasons.

CUS	Client untrusted server	The client did not have an entry in its known_hosts file for this server.
RSP	Reverse SSH Provisioned	The client connected with a -R flag, which provisions the ports to be used for a Reverse Session set up at any future time.
RSI	Reverse SSH Initiated	The Reverse session is initiated from the server back to the Client.
RSIA	Reverse SSH Initiation Automated	The initiation of the Reverse session happened very early in the packet stream, indicating automation.
RSL	Reverse SSH Logged In	The Reverse tunnel login has succeeded.
RSK	Reverse SSH Keystrokes	Keystrokes are detected within the Reverse tunnel.
NRC	No Remote Command	The -N flag was used in the SSH session.
AFR	SSH Agent Forwarding Requested	Agent forwarding is requested by the Client.

The C2 Collection

Packages

Package	Description
DGA Detection	Identifies potentially malicious traffic on your network by flagging DNS activity that's likely associated with a known Domain Generation Algorithm (DGA).
DNS Tunnels	Detects both specific and generic DNS tunnels.
HTTP C2	Flags select command and control (C2) patterns in HTTP traffic on your network.
ICMP Tunnels	Detects both specific and generic ICMP tunnels.
Meterpreter Detection	Identifies Meterpreter-formatted headers in TCP connections and creates a meterpreter.log. When a header is specifically detected through analysis of a TCP header, the package extracts more detailed information from that header and reports it in a separate meterpreter_headers.log

Notices

DGA

- DGA::Infected_Host_Activity

DNS Tunneling

- generic_dns_tunnel::GenericDNSTunnel
- DNSTunnel::Detected (Iodine)
- DNSTunnel::Detected (sods)
- DNSTunnel::Detected (TUNS)
- DNSTunnel::Detected (DNScat)
- DNSTunnel::Detected (Dns2tcp)
- DNSTunnel::Detected (Your Freedom)

ICMP Tunneling

- generic_icmp_ping_tunnel::ICMP_PING_TUNNEL
- ICMPSpecificTunnelDetectors:: (Hans)
- ICMPSpecificTunnelDetectors:: (ICMP Shell)
- ICMPSpecificTunnelDetectors:: (icmpsh)
- ICMPSpecificTunnelDetectors:: (ICMPTX)
- ICMPSpecificTunnelDetectors:: (ITun)
- ICMPSpecificTunnelDetectors:: (PingTunnel)

HTTP C2

- HTTP_C2::C2_Traffic_Observed (Azorult)
- HTTP_C2::C2_Traffic_Observed (Chisel)
- HTTP_C2::C2_Traffic_Observed (Cobalt Strike)
- HTTP_C2::C2_Traffic_Observed (Drovorub)
- HTTP_C2::C2_Traffic_Observed (Emotet)
- HTTP_C2::C2_Traffic_Observed (Empire)
- HTTP_C2::C2_Traffic_Observed (Houdini)
- HTTP_C2::C2_Traffic_Observed (Icedid)
- HTTP_C2::C2_Traffic_Observed (Meterpreter)
- HTTP_C2::C2_Traffic_Observed (Pupy)
- HTTP_C2::C2_Traffic_Observed (Qbot/qakbot)
- HTTP_C2::C2_Traffic_Observed (sshorty)
- HTTP_C2::C2_Traffic_Observed (Zbot)

corelight

Defenders have always sought the high ground in order to see farther and turn back attacks. Corelight delivers a commanding view of your network so you can outsmart and outlast adversaries. We capture, interpret, and connect the data that means everything to defenders.

info@corelight.com | 888-547-9497