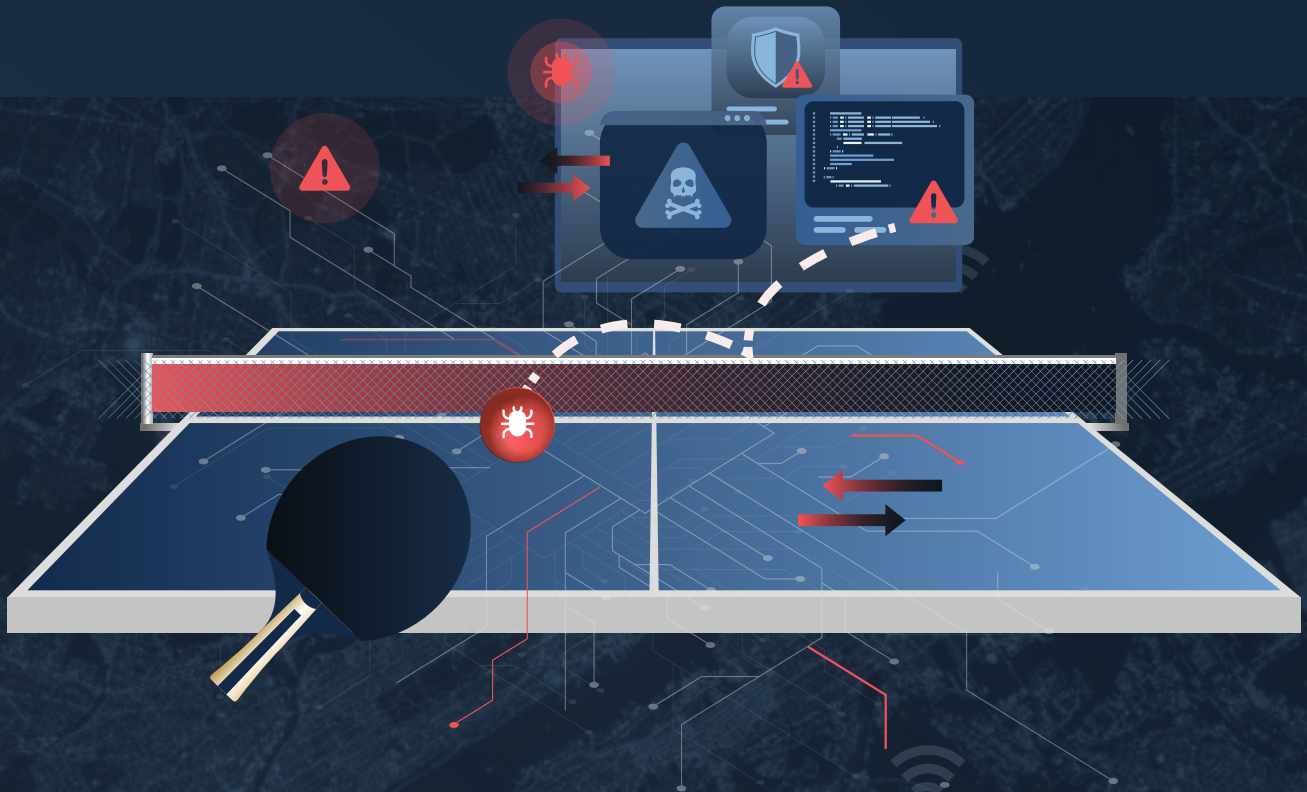


Cynamics Revealing - Using Malicious Pings for C&C and Data Leakage

www.cynamics.ai | info@cynamics.ai



At Cynamics, we're building the impossible: inferring 100% of a network by analyzing just 1% of its traffic samples, using unique patented AI technology. We help municipalities, critical infrastructure, healthcare, and other highly complex and sensitive organizations predict and prevent attacks and optimize network performance.

In this case study, we'll describe a recent attack vector detected in several of our customers related to malicious ping packets. We haven't found any prior indication for such an attack vector. Ping is one of the basic building blocks of the internet, used to test the reachability of a host. It is available for virtually all operating systems that have networking capability, including network administration software .⁽¹⁾

Ping operates by sending Internet Control Message Protocol (ICMP) echo request packets to the target host and waiting for an ICMP echo reply. The program can then report errors, packet loss, and a statistical summary of the results, typically including minimum, maximum, mean round-trip times, and standard deviation of the mean.

1 https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol

2 [https://en.wikipedia.org/wiki/Ping_\(networking_utility\)](https://en.wikipedia.org/wiki/Ping_(networking_utility))

The ICMP packet is very simple:

	Bits 0–7	Bits 8–15	Bits 16–23	Bits 24–31
Header (20 bytes)	Version/IHL	Type of service	Length	
	Identification		flags and offset	
	Time To Live	Protocol	Header Checksum	
	Source IP address			
	Destination IP address			
	ICMP Header (8 bytes)	Type of message	Code	Checksum
Header Data				
ICMP Payload (optional)	Payload Data			

Figure 1: ICMP packet datagram (2)

IPv4 Header (in blue):

- Protocol is set to 1
- Source-IP and Destination-IP addresses

ICMP Header (in red):

- Type of ICMP message (8 bits)
- Code (8 bits)
- Checksum (16 bits)
- Header Data (32 bits) field, which in this case (ICMP echo request and replies), will be composed of identifier (16 bits) and sequence number (16 bits).

Very simple, right?

Seems like there is nothing to manipulate...

so basic, that many organizations keep it open to the world.


But it's not. Dynamics recently detected malicious usage of allegedly innocent ping packets for Command and Control (C&C) and data leakage in some of our public sector and government customers. This was done by using ping packets with unusual port numbers, which usually don't contain either source or destination ports.

Still, there are a few cases where firewalls encode the ping type/code as source or destination ports, such as:




In Fortigate

the destination-port field is used to report ICMP code. (3)



In Juniper

the source-port is used for the ICMP Sequence Number and the destination-port for the ICMP Identifier. (4)



In Cisco

the destination-port is displaying the ICMP Code and the source-port is displaying the ICMP type. (5)



Notice that in the latter two cases, both source and destination ports should be explicit, i.e., not empty (Null).

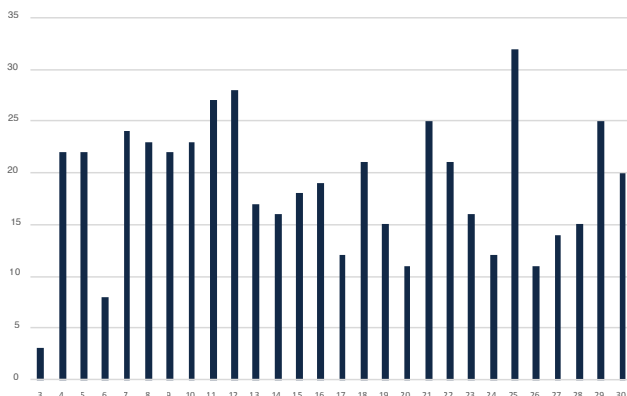
Furthermore, the port values should be up to 255, as ICMP types/codes are limited by 8 bits. (6) In several customers, we recently detected usage of ping packets, both in internal and external communications, associated with either source-port or destination-port (not both), with values ranging from 256 to ten-thousands, **which doesn't follow any RFC, vendor documentations and Internet Protocols standards.**

The Dynamics Analysis:

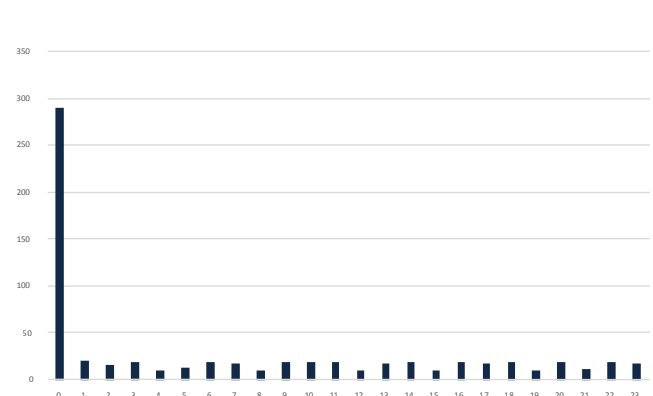
One third of this traffic was completely internal (internal IP <-> internal IP), and the main IPs were associated with active-directory servers.

The communication was throughout all day - low-volume and stealth looking, but had a significant spike at midnight:

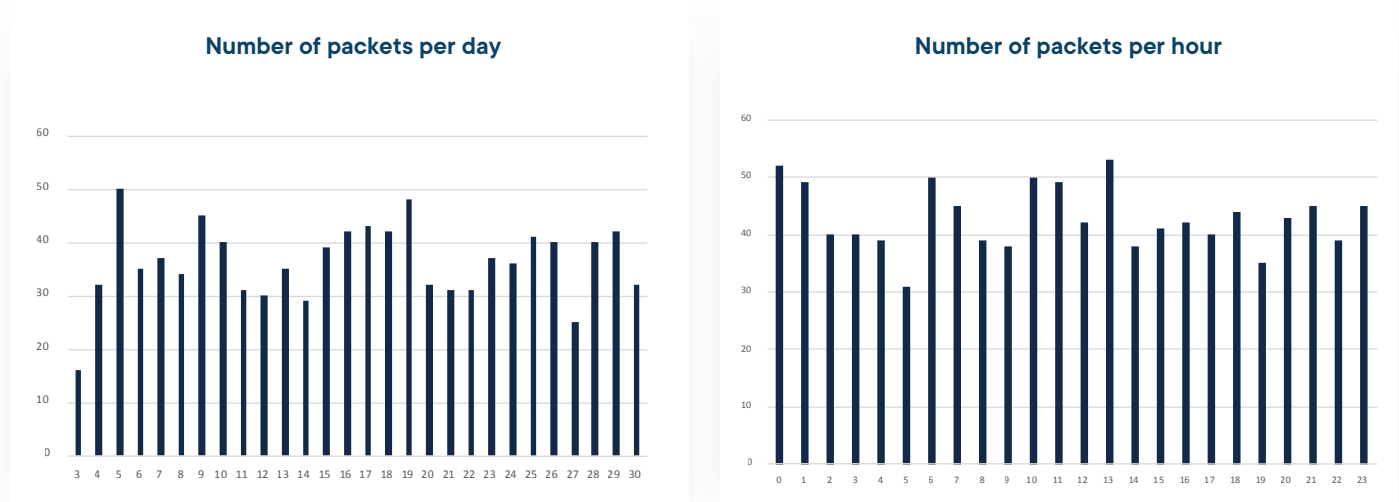
Number of packets per day



Number of packets per hour



All external traffic was with servers in the DMZ, both inbound and outbound. Unlike internal communication, external communication was uniformly distributed throughout the month and day. In addition, the port numbers were random:



Connecting the dots, due to the low volume and small average size of packets (a few dozen bytes), it is less likely to be part of data leakage. Instead, our assessment is that the communication was part of Command and Control keep-alive between various infected machines and the attacker.

Notice the use of the active-directory internally and DMZ externally, which are well suited for a sophisticated attacker looking to expand his footprint and propagate internally, and covering himself by communication with the DMZ through a diverse set of external IP addresses.



- <https://kb.fortinet.com/kb/documentLink.do?externalID=FD34359>
- <https://kb.juniper.net/InfoCenter/index?page=content&id=KB5116&pmv=print>
- https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/working_with_intrusion_events.html
- <https://tools.ietf.org/html/rfc792>

Using such malicious pings, an attacker can do the following:

1 Scan and map your target network prior to an attack:

- a. This is an initial step for almost every attack - by sending pings to various different internal IPs, the attacker could map your target network, which servers are up, and what IP addresses are used.
- b. After mapping your network, the attacker can further check for open ports, to match with known vulnerabilities.




2 Command and Control (C&C) communication:

- a. once gaining a footprint to your network, the attacker can use the pings to send commands from outside and keep-alives from the inside, covering himself by using low volume traffic from a diverse set of IP addresses.

3 Data leakage

- a. The attacker can further use this communication channel to attach payload to the ping packets and leak data outside.

Mitigation

-  • In general, always block ICMP traffic from external sources, unless for very specific whitelisted IPs with a very good reason.
-  • Block ICMP traffic with port numbers bigger than 255, as they are not expected in any RFC, vendor documentations, or Internet Protocols standards.
-  • If you do detect such traffic, immediately update credentials and verify patching in every server that communicates with such pings.

**Use Cynamics today to uncover malicious pings,
as well as gain complete network visibility and
threat prediction to your network.**