Cynamics

Cynamics Revealing-

“Known-To-Known” Communications

Whitepaper

cynamics.ai

A New Attack Vector

Recently, Cynamics AI revealed a new, previously unknown sophisticated attack vector. We call it “known-to-known” attacks, as it uses communications where both the source-port and dest-port are “well-known” services, for example, a connection with source-port being SSH (22) and destination-port being HTTP (80).

As we all learned in Networking 101, most internet services operate in a client-server model where the server uses a well-known port (e.g., SSH or HTTP), and the client uses a register or dynamic 5-digit port value, which is randomly selected (e.g., 55344). Therefore, connections where both port sides are from the well-known range do not follow TCP/IP suite and standards or protocols RFC, and are detected by Cynamics as being related to malicious operations at various clients in very different industries.

It’s important to emphasize we are not referring to specific “special cases” that such known-to-known ports combinations are allowed by the protocols RFCs, such as in NTP (123)[1]; Syslog (514), and other services, where both the source-port and dest-port can be the same value. We are referring only to cases where the combination of the source-port and the dest-port is “impossible,” such as HTTP with DNS in the same connection, etc.

The ports range definition[2]

The well-known range (0-1024), mainly dedicated for fundamental and highly recognised services and protocols, such as DNS, HTTP/s, SMTP and many more. Each service has been assigned with a discrete number of ports (usually around two ports). Even in some operating systems the usage of this range is locked and could only be accessed by the root user. This is unlike the dynamic ports range (49152-65535) which is usually not related to any specific service (none of the ports from this range could be assigned to an application) and should be associated with the client in the server-client model. The purpose of the registered ports range stands in the middle, it should be used for applications and service by assigning the ports by a requesting entity, but it could also be used as client ports.[3][4]

1 https://www.rfc-editor.org/rfc/rfc5905.html , page 32

2 https://datatracker.ietf.org/doc/html/rfc6335

3 https://www.geeksforgeeks.org/bind-port-number-less-1024-non-root-access/

4 While this range is mainly used for client ports, it might be also used for private or customized services.

Connections where both source and destination ports are from the well-known range do not follow the intended purpose of these ranges as described in the RFC and the expected client-server model. Therefore, they are suspicious and may be the result of a malicious attack.

About the attack

As a team of experienced security professionals, this behavior raised our curiosity, so when the Cynamics AI technology picked it up in various clients of different geographies, industries, sizes, and other characteristics, we understood we were witnessing a novel attack vector. We assume that these communications are a type of "smart pin-pointed attack," where instead of broad port scanning and searching for open/allowed ports and risking being detected, in this novel attack vector each communication is a bi-fold attempt to trick the firewall and bypass it. By trying both ports to be of known services that are commonly used or left open, it increases the chances that one of them will be allowed. Usually, firewalls block communications per ports or IPs/subnets but are not looking at the combination between the ports. In well-known communications both ports are legit, so it makes sense that these ports or at least one of them will be open in one of the directions. On the other hand, a port scan is noisier, easily detected and only searching for open services on the destination, so most of the firewalls block it in some way (either by rules on closed ports or by heuristics). Other ways this attack might be utilized is to trick the attacked device to communicate with another service on the attacker or the attacked device might start to listen to an unintended port.[5]

We are seeing these attacks every day in many clients at different settings: north-south, inbound and outbound traffic, and even east-west inside the organization network. Usually, these attacks were associated with low volume, stealth-looking communications. We therefore believe attackers can use this for C&C purposes and also for covering the true content of the packet, penetrating the network, infecting devices, propagating, and hopping between devices - and even focussing on small data leakages. It might also be used for accessing internal services that should not be accessible by leveraging the other port side, which might be allowed.

Cynamics to the rescue

Cynamics's approach is the answer to the known-to-known communications problem. With its complete network visibility and coverage, our technology analyzes network patterns around the full 5-tuple[6] connections (and not just per port or IP like legacy NDR solutions) and detects these suspicious behaviors as their patterns are significantly unusual.

Let's look at some detection examples.

---

5 For example, https://www.rfc-editor.org/rfc/rfc7231.html , page 31

6 The connection ID consists of the source IP address and port, destination IP address and port, and IP protocol.

Case studies examples

The first example is from a large US hospital chain. In July 2022, Cynamics detected two new outbound communications between one of their CRMs, where their ports were from the well-known range on both sides. In these two communications, one of the ports was HTTP[7] (port 80), which is open on the CRM, so the attacker knew it would reply to him. The ports on the other side were also from the well-known range. When we looked for these IPs, we discovered that one of them is highly malicious (for example, see its record below in the highly credible reputation source of Virus-Total[8]). Moreover, both of the destination ports are assigned by IANA for different usage and have been abused by trojans in the past (Doly and SynDrop trojans)

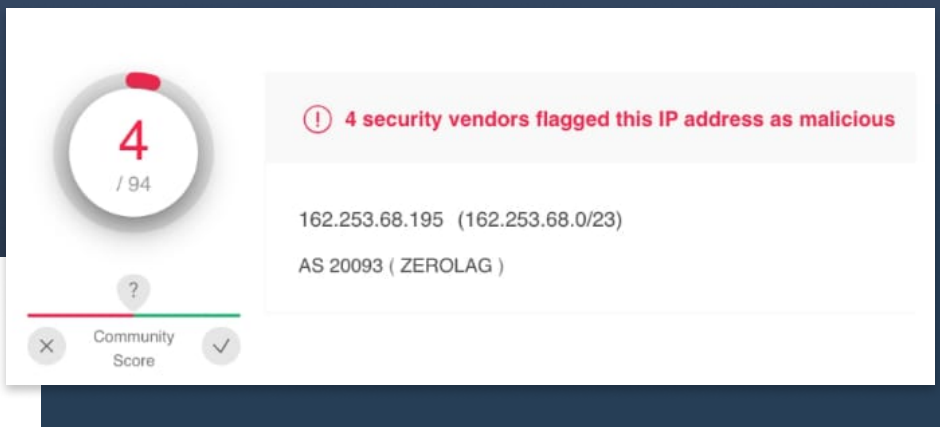

Figure 1: Virus-Total indications of malicious activities of 162.253.68.195

Source IP	Destination IP	Source Port	Destination Port	Destination Country	Destination Organization	Total Packets	Length (bytes)
172.24.146.84	162.253.68.195	80	1010	United States	ZeroLag Communications	100	175
	20.29.127.41	80	3	United States	Microsoft	100	68

The second one is from a US-based global construction company. It was just a month ago when Cynamics detected many inbound known-to-known communications, in addition to one outbound communication from internal IP to the world. In this connection, the port on the internal side was 443 (HTTPs) and on the public side, port 3. When we checked the public IP, we discovered it to be also highly malicious (for example, see below from Virus-Total). Based on Cynamics' detection, **the IT team inspected this internal endpoint 10.1.10.14 and found malicious processes running on it.**

7 As HTTP isn't encrypted, the best practice is switching to secure HTTPs communications.

8 https://www.virustotal.com/

Source IP	Destination IP	Source Port	Destination Port	Destination Country	Destination Organization	Total Packets	Length (bytes)
10.1.10.14	45.61.188.138	443	3	United States	FranTech Solutions	100	60

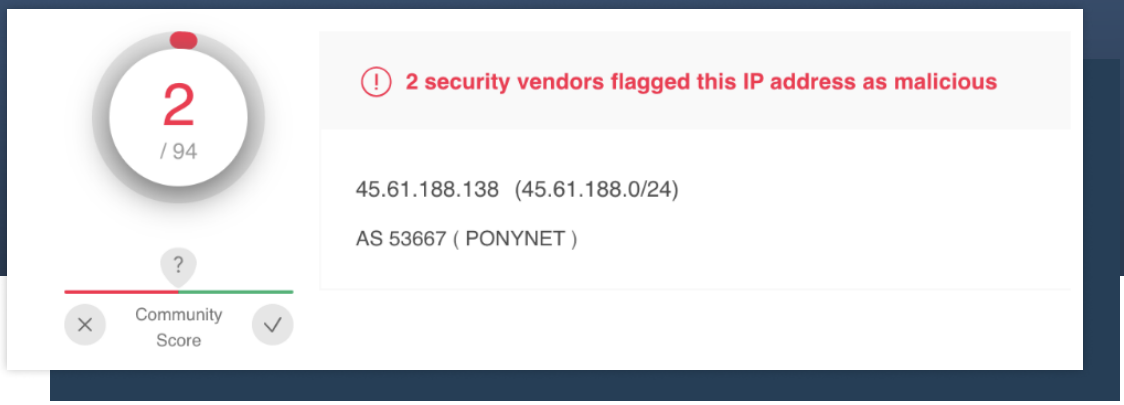

Figure 2: Virus-Total indications of malicious activities of 45.61.188.138

It's important to emphasize that in both cases above, the detections were not based on flagging these IPs as malicious, but on the Cynamics AI analyzing the network patterns and detecting this suspicious, unusual pattern of both source and destination ports being "well-known". Only after we cross-checked these detected IPs we found out about their malicious indications, even before the malicious IPs were flagged by other security researchers. **This demonstrates Cynamics' ability to detect malicious communications based on their network patterns.**

The final example is from a mid-size service provider: Cynamics detected many known-to-known communications between their network and the world (see Figure 3 below). Following Cynamics' detection of these network-wide suspicious behaviour, **the client's cybersecurity team found several ransomware time-bombs in several of the endpoints flagged by Cynamics,** showing these known-to-known communications might have been C&C keep-alive traffic from these infected machines outside to the attacker premises. There are also internal communications over these ports which might be an internal propagation.

Indeed, some of these network communications were with unusual organizations and countries that this client had nothing to do with, and some of the IPs were highly malicious (see below from Virus-Total). In spite of that, these attacks could originate from legitimate and highly communicated ISP, hosting and cloud companies, which without this detection may not be found. In this case study, there was an attack from an AWS EC2 machine (54.208.32.172).

Source Port	Destination Port	Source IPs	Destination IPs	Source Countries	Destination Countries	Volume	Total Packets
21	21	[redacted]	[redacted]	United States, United Kingdom, Netherlands, China, Portugal, Turkey, Singapore, Brazil, France	United States, Indonesia, France, Portugal, Turkey, South Korea, Singapore, Brazil, United Kingdom	2.12K	981.40K
80	21	168.205.53.254	[redacted]	Brazil	United States	46	100
514	1022	10.20.9.5	10.20.4.5	–	–	1.49K	2.70K
829	23	190.52.128.159	[redacted]	Paraguay	United States	46	100
1017	1020	10.20.4.5	10.20.9.5	–	–	92	200

Figure 3: Cynamics VCA (Virtual Cyber Analyst) detections of the known-to-known communications, notice the source and destination ports in the two columns on left

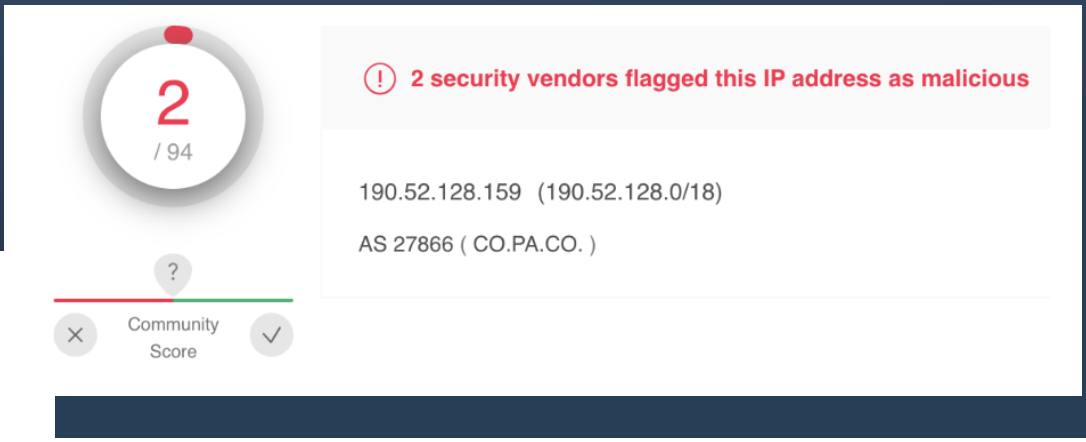

Figure 4: Virus-Total indications of malicious activities of 190.52.128.159

Preventing known-to-known communications

First, when you detect communications like this in your network, block them immediately and inspect your endpoints for possible compromises, even if the connections are only internal.
Second, if possible by your firewall, we recommend closing all the port combinations of two well-known. If not, block unnecessary ports in the firewall, especially from the well-known range. In this way, we can reduce the chance that the attacker will succeed in creating a connection with two ports that open in the firewall.

However, these steps are just the beginning. To get full and immediate protection from this attack and many other threats and malicious campaigns, as well as full network coverage, start your Cynamics POC today.