October 14, 2014

2 Comments

Threat Research

Threat Spotlight: Group 72

Talos Group

This post is co-authored by Joel Esler, Martin Lee and Craig Williams

Everyone has certain characteristics that can be recognised. This may be a way of walking, an accent, a turn of phrase or a style of dressing. If you know what to look for you can easily spot a friend or acquaintance in a crowd by knowing what characteristics to look for. Exactly the same is true for threat actors.

Each threat actor group may have certain characteristics that they display during their attack campaigns. These may be the types of malware that they use, a pattern in the naming conventions of their command and control servers, their choice of victims etc. Collecting attack data allows an observer to spot the characteristics that define each group and identify specific threat actors from the crowd of malicious activity on the internet.

Talos security and intelligence research group collects attack data from our various telemetry systems to analyse, identify and monitor threat actors through their different tactics, techniques, and procedures. Rather than give names to the different identified groups, we assign numbers to the threat actors. We frequently blog about significant attack campaigns that we discover, behind the scenes we integrate our intelligence data directly into our products. As part of our research we keep track of certain threat actor groups and their activities. In conjunction with a number of other security companies, we are taking action to highlight and disrupt the activities of the threat actors identified by us as Group 72.

Group 72 is a long standing threat actor group involved in Operation SMN, named Axiom by Novetta. The group is sophisticated, well funded, and possesses an established, defined software development methodology. The group targets high profile organizations with high value intellectual property in the manufacturing, industrial, aerospace, defense, media sectors. Geographically, the group almost exclusively targets organizations based in United States, Japan, Taiwan, and Korea. The preferred tactics of the group include watering-hole attacks, spear-phishing, and other web-based tactics.

The tools and infrastructure used by the attackers are common to a number of other threat actor groups which may indicate some degree of overlap. We have seen similar patterns used in domain registration for malicious domains, and the same tactics used in other threat actor groups leading us to believe that this group may be part of a larger organization that comprises many separate teams, or that different groups share tactics, code and personnel from time to time.

It is possible that Group 72 has a vulnerability research team searching for 0-day vulnerabilities in Windows. The group is associated with the initial attack campaigns utilising exploits for the following vulnerabilities CVE-2014-0322 and CVE-2012-4792 . We have also observed them using SQL injection as part of their attacks, and exploits based on CVE-2012-1889 and CVE-2013-3893.

Frequently the group deploys a remote access trojan (RAT) on compromised machines. These are used both to steal data and credentials from compromised machines, and to use the machine as a staging post to conduct attacks against further systems on the network, allowing the attackers to spread their compromise within the organization. Unlike some threat actors, Group 72 does not prefer to use a single RAT as part of their attacks. We have observed the group to use the following RAT malware:

- Gh0st RAT (aka Moudoor)
- Poison Ivy (aka Darkmoon)
- HydraQ (aka 9002 RAT aka McRAT aka Naid)
- Hikit (aka Matrix RAT aka Gaolmay)
- Zxshell (aka Sensode)
- DeputyDog (aka Fexel) – Using the kumanichi and moon campaign codes
- Derusbi
- PlugX (aka Destroy RAT aka Thoper aka Sogu)
- HydraQ and Hikit, according to our data are unique to Group 72 and to two other threat actor groups.

While their operational security is very good, patterns in their domains can be identified such as seemingly naming domains after their intended victim. We have observed domains such as *companyname.attackerdomain.com* and *companyacronym.attackerdomain.com*. We have also observed similar patterns in the disposable email addresses used to register their domains. These slips, among others, allow us to follow their activities. Intriguingly we have observed the same email address being used in the activities of this and two other threat actor groups. This may suggest that these three groups are indeed one unit, or possibly hint at shared staff or ancillary facilities.

We will post a follow up with more technical detail in the coming days.

ClamAV names and Snort Signature IDs detecting Group 72 RAT malware:

- Gh0stRat – Win.Trojan.Gh0stRAT, 19484, 27964
- PoisonIVY / DarkMoon – Win.Trojan.DarkMoon, 7816, 7815, 7814, 7813, 12715, 12724
- Hydraq – Win.Trojan.HyDraq, 16368, 21304
- HiKit – Win.Trojan.HiKit, 30948
- Zxshell – Win.Trojan.Zxshell, 32180, 32181
- DeputyDog – Win.Trojan.DeputyDog, 28493, 29459
- Derusbi – Win.Trojan.Derusbi, 20080

Protecting Users Against These Threats

Product	Protection
AMP	✓
CWS	✓
ESA	✓
Network Security	✓
WSA	✓

Advanced Malware Protection (AMP) is ideally suited to detect the sophisticated malware used by this threat actor.

CWS or WSA web scanning prevents access to malicious websites, including watering hole attacks, and detects malware used in these attacks.

The Network Security protection of IPS and NGFW have up-to-date signatures to detect malicious network activity by threat actors.

ESA can block spear phishing emails sent by threat actors as part of their campaign.

Tags: APT malware Operation SMN security SMN Talos threats

2 Comments

Blake VandeVelde says:

November 3, 2014 at 12:43 pm

I see mention made of "The Network Security protection of IPS and NGFW have up-to-date signatures to detect malicious network activity by threat actors." There are four CVE's listed in this article, and I only see two of them (the ones from 2012) showing up in the ASA CX IPS product. None of the other threat names show up in the ASA CX IPS either. We have the latest Oct 2014 signatures.

Based on this document, (http://www.cisco.com/c/en/us/products/security/asa-5500-series-next-generation-firewalls/eos-eol-notice-listing.html) ASA CX is not EOL, so there ought to be regular IPS signatures coming out to protect us against things like this. When will we be protected against these threats?

Alex Chiu says:

November 3, 2014 at 3:01 pm

Blake,

Cisco CX IPS is not designed to address the entire range of signatures offered by the Cisco IPS. It is targeted for specific deployments and runs a subset of the signatures from the Cisco IPS. Each new IPS signature is evaluated, and when possible, implemented on CX.

If you have any further questions on CX signature coverage feel free to reach out to ips-signature-team@cisco.com.

Comments are closed.