Tracking Tick Through Recent Campaigns Targeting East Asia

By Ashlee Benge

Published: 2018-10-18 · Archived: 2026-04-05 23:20:53 UTC

Summary

Since 2016, an advanced threat group that Cisco Talos is tracking has carried out cyberattacks against South Korea and Japan. This group is known by several different names: Tick, Redbaldknight and Bronze Butler.

Although each campaign employed custom tools, Talos has observed recurring patterns in the actor's use of infrastructure, from overlaps in hijacked command and control (C2) domains to differing campaign C2s resolving to the same IP. These infrastructure patterns indicate similarities between the Datper, xxmm backdoor, and Emdivi malware families. In this post, we will dive into these parallels and examine the methods used by this actor.

Introduction

The APT threat actor known as "Tick," "Bronze Butler," and "Redbaldknight" has conducted espionage campaigns since 2016 against East Asian countries such as Japan and South Korea [1]. Talos analyzed a recent campaign in which compromised websites located in South Korea and Japan were used as C2 servers for samples belonging to the malware family known as "Datper," which has the ability to execute shell commands on the victim machine and obtain hostnames and drive information. Talos found potential links in shared infrastructure between the malware families Datper, xxmm backdoor, and Emdivi, each of which has been attributed to this threat actor under one of the above three aliases.

We obtained this Datper variant through VirusTotal. The sample, written in Delphi code, was submitted toward the end of July 2018. Although the exact attack vector is unclear, the threat actor appears to have selected a legitimate-but-vulnerable Korean laundry service website to host their C2, shown below.

Legitimate Korean laundry site used as Datper C2 host. The website, located at whitepia[.]co.kr, does not use SSL encryption or certificates. The specific URL used for C2 communication is:

hxxp://whitepia[.]co[.]kr/bbs/include/JavaScript.php

Once executed, the Datper variant creates a mutex object called "gyusbaihysezhrj" and retrieves several pieces of information from the victim machine, including system information and keyboard layout. Afterward, the sample attempts to issue an HTTP GET request to the above C2 server, which at the time of this writing, resolved to the IP 111[.]92[.]189[.]19.

An example of this request is:

GET /bbs/include/JavaScript.php?ycmt=de4fd712fa7e104f1apvdogtw HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: whitepia[.]co.kr
Cache-Control: no-cache

Unfortunately, at the time of this investigation, the C2 server was unavailable, preventing Talos from investigating C2 communications in greater detail. However, Talos was able to analyze a previous campaign from 2017, which employed a similar sample from this family and used a slightly different mutex, "d4fy3ykdk2ddssr." All samples in the diagram below, associated with the 2017 campaign, implemented mutex object "d4fy3ykdk2ddssr," likely to prevent access from other processes during execution.

Structure of C2 communications from the 2017 campaign. The actor behind this campaign deployed and managed their C2 infrastructure mainly in South Korea and Japan. We confirmed that the actor periodically changed their C2 infrastructure and appears to have a history of identifying and penetrating vulnerable websites located in these countries. In addition to whitepia[.]co[.]kr, we identified other instances of compromised websites used as C2 servers. It is possible the malware samples are being delivered using web-based attacks, such as drive-by downloads or watering hole attacks. Additionally, Talos identified hosts used as C2 servers that may not be connected to a compromised website. This indicates the possibility that the threat actor may have initially deployed their C2 server infrastructure on legitimately obtained (and potentially purchased) hosts.

Overlaps in the compromised websites used as C2 domains suggest links to another malware family known as "xxmm backdoor" (or alternatively, "Murim" or "Wrim"), a malware family that allows an attacker to install additional malware. The GET request URI paths of xxmm backdoor and Datper are similar, as seen below:

xxmm backdoor: hxxp://www.amamihanahana.com/diary/archives/a_/2/index.php

Datper: hxxp://www.amamihanahana.com/contact/contact_php/jcode/set.html

Based on the findings above, both tools have used the same websites located in Japan in their C2 infrastructure since 2016.

The xxmm sample, shown on the right-hand side of the diagram above, has the hash 397a5e9dc469ff316c2942ba4b503ff9784f2e84e37ce5d234a87762e0077e25 [2].

The extracted PDB debug symbol paths from the sample are:

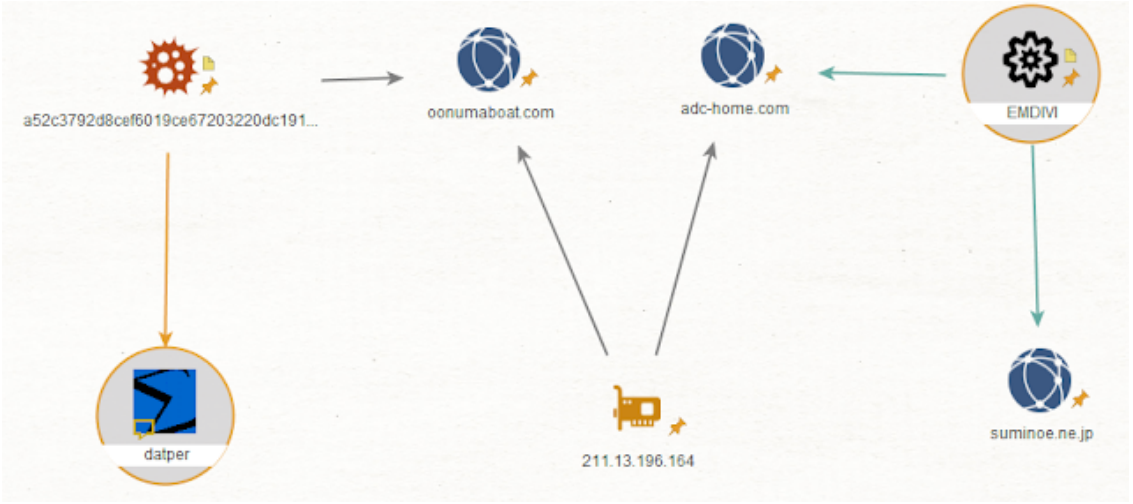
C:\Users\123\Documents\Visual Studio 2010\Projects\shadowWalker\Release\BypassUacDll.pdb

C:\Users\123\Documents\Visual Studio 2010\Projects\shadowWalker\Release\loadSetup.pdb

C:\Users\123\documents\visual studio 2010\Projects\xxmm2\Release\test2.pdb

C:\Users\123\Desktop\xxmm3\x64\Release\ReflectivLoader.pdb

In addition to the links between Datper and xxmm backdoor, a recent Datper variant compiled in March 2018 used a legitimate website as a C2, which resolved to the IP 211[.]13[.]196[.]164. This same IP was used as C2 infrastructure by the Emdivi malware family — a trojan that opens a backdoor on the compromised machine — and was attributed to the threat actor behind the campaign "Blue termite" [3].



Structure of 2018 Datper and Emdivi campaigns. Our passive DNS lookup data of Resource Records (RR) for domains used by Datper and Emdivi further suggest that this IP was used by both malware families.

RR Name	RR Type	RData	Time First Seen	Time Last Seen
www[.]oonumaboat[.]com	A	211[.]13.196.164	10/31/2016 14:20	8/27/2017 23:21
www[.]oonumaboat[.]com	A	211[.]13.196.164	9/30/2017 20:51	10/4/2018 8:59

Resource record for Datper.

RR Name	RR Type	RData	Time First Seen	Time Last Seen
www[.]adc-home[.]com	A	211[.]13.196.164	5/17/2017 0:49	8/31/2017 10:32
www[.]adc-home[.]com	A	211[.]13.196.164	9/1/2017 12:22	9/27/2018 8:57

Resource record for Emdivi.

Conclusion

Talos' investigation into attacks conducted by this actor indicates commonalities between the Datper, xxmm backdoor, and Emdivi malware families. Specifically, these similarities are in the C2 infrastructure of attacks utilizing these malware families. Some C2 domains used in these attacks resolve to hijacked, legitimate South Korean and Japanese hosts and may have been purchased by the attacker. Successful attacks utilizing these malware families may result in shell commands being run on victim machines, resulting in a potential leak of sensitive information. Cisco security products protect our customers in a range of ways, detailed below.

Coverage

Additional ways our customers can detect and block this threat are listed below.

PRODUCT	PROTECTION
AMP	✔
CloudLock	N/A
CWS	✔
Email Security	✔
Network Security	✔
Threat Grid	✔
Umbrella	✔
WSA	✔

Advanced Malware Protection (AMP) is ideally suited to prevent the execution of the malware used by these threat actors.

Cisco Cloud Web Security (CWS) or Web Security Appliance (WSA) web scanning prevents access to malicious websites and detects malware used in these attacks.

Email Security can block malicious emails sent by threat actors as part of their campaign.

Network Security appliances such as Next-Generation Firewall (NGFW), Next-Generation Intrusion Prevention System (NGIPS), and Meraki MX can detect malicious activity associated with this threat.

AMP Threat Grid helps identify malicious binaries and build protection into all Cisco Security products.

Umbrella, our secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs, and URLs, whether users are on or off the corporate network.

Open Source SNORT® Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

IOCs:

Hashes

Datper

c2e87e5c0ed40806949628ab7d66caaf4be06cab997b78a46f096e53a6f49ffc

569ceec6ff588ef343d6cb667acf0379b8bc2d510eda11416a9d3589ff184189

d91894e366bb1a8362f62c243b8d6e4055a465a7f59327089fa041fe8e65ce30

5a6990bfa2414d133b5b7b2c25a6e2dccc4f691ed4e3f453460dee2fbbcf616d

7d70d659c421b50604ce3e0a1bf423ab7e54b9df361360933bac3bb852a31849

2f6745ccebf8e1d9e3e5284a895206bbb4347cf7daa2371652423aa9b94dfd3d

4149da63e78c47fd7f2d49d210f9230b94bf7935699a47e26e5d99836b9fdd11

a52c3792d8cef6019ce67203220dc191e207c6ddbdfa51ac385d9493ffe2a83a

e71be765cf95bef4900a1cef8f62e263a71d1890a3ecb5df6666b88190e1e53c

xxmm backdoor

397a5e9dc469ff316c2942ba4b503ff9784f2e84e37ce5d234a87762e0077e25

Emdivi

9b8c1830a3b278c2eccb536b5abd39d4033badca2138721d420ab41bb60d8fd2

1df4678d7210a339acf5eb786b4f7f1b31c079365bb99ab8028018fa0e849f2e

IPs used for C&C communication

202[.]218[.]32[.]135

202[.]191[.]118[.]191

110[.]45[.]203[.]133

61[.]106[.]60[.]47

52[.]84[.]186[.]239

111[.]92[.]189[.]19

211[.]13[.]196[.]164

C&C servers resolving to malicious IPs

hxxp://www.oonumaboat[.]com/cx/index.php
hxxp://www.houeikai[.]or.jp/images/ko-ho.gif

hxxp://www.amamihanahana[.]com/contact/contact_php/jcode/set.html

hxxp://www.amamihanahana[.]com/diary/archives/a_/2/index.php

hxxp://rbb.gol-unkai4[.]com/common/include/index-visual/index.htm

hxxp://www.whitepia[.]co.kr/bbs/include/JavaScript.php

hxxp://www.adc-home[.]com/28732.html

hxxp://www.sakuranorei[.]com.com/blog/index.php

Source: https://blog.talosintelligence.com/2018/10/tracking-tick-through-recent-campaigns.html