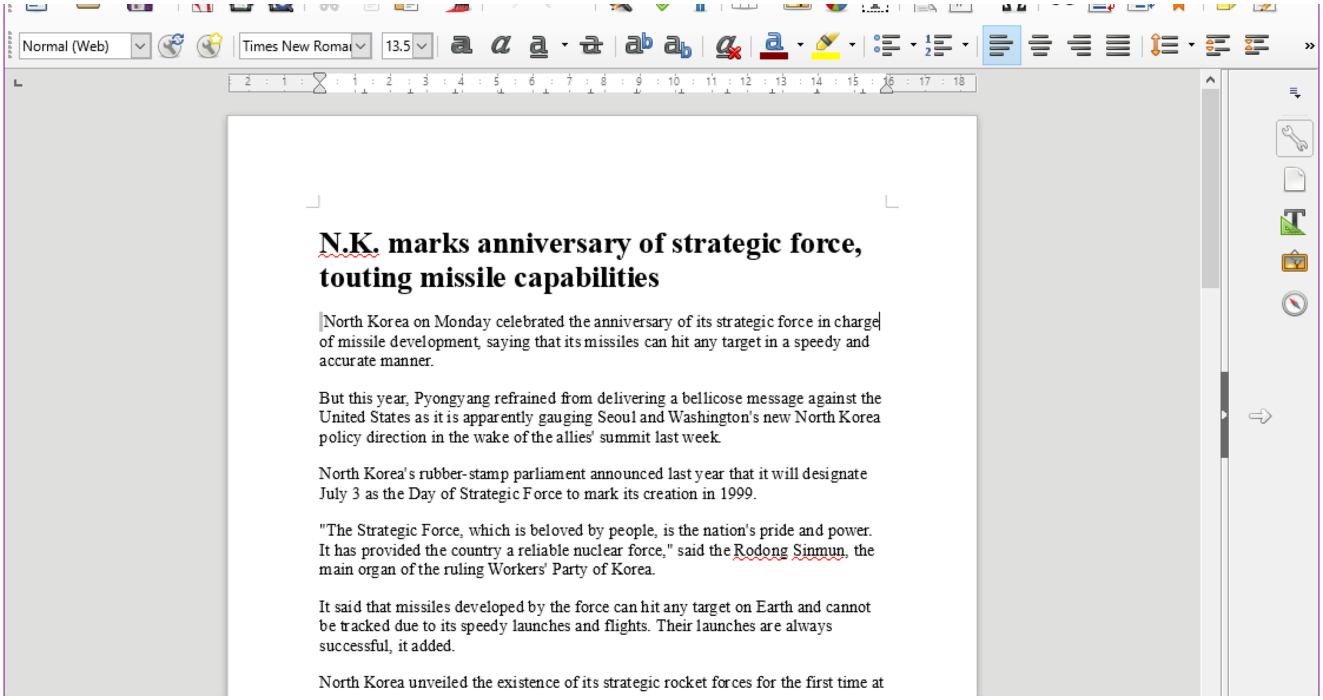
New KONNI Campaign References North Korean Missile Capabilities

blog.talosintelligence.com/2017/07/konni-references-north-korean-missile-capabilities.html



N.K. marks anniversary of strategic force, touting missile capabilities

North Korea on Monday celebrated the anniversary of its strategic force in charge of missile development, saying that its missiles can hit any target in a speedy and accurate manner.

But this year, Pyongyang refrained from delivering a bellicose message against the United States as it is apparently gauging Seoul and Washington's new North Korea policy direction in the wake of the allies' summit last week.

North Korea's rubber-stamp parliament announced last year that it will designate July 3 as the Day of Strategic Force to mark its creation in 1999.

"The Strategic Force, which is beloved by people, is the nation's pride and power. It has provided the country a reliable nuclear force," said the Rodong Sinmun, the main organ of the ruling Workers' Party of Korea.

It said that missiles developed by the force can hit any target on Earth and cannot be tracked due to its speedy launches and flights. Their launches are always successful, it added.

North Korea unveiled the existence of its strategic rocket forces for the first time at

This blog was authored by Paul Rascagneres

Executive Summary

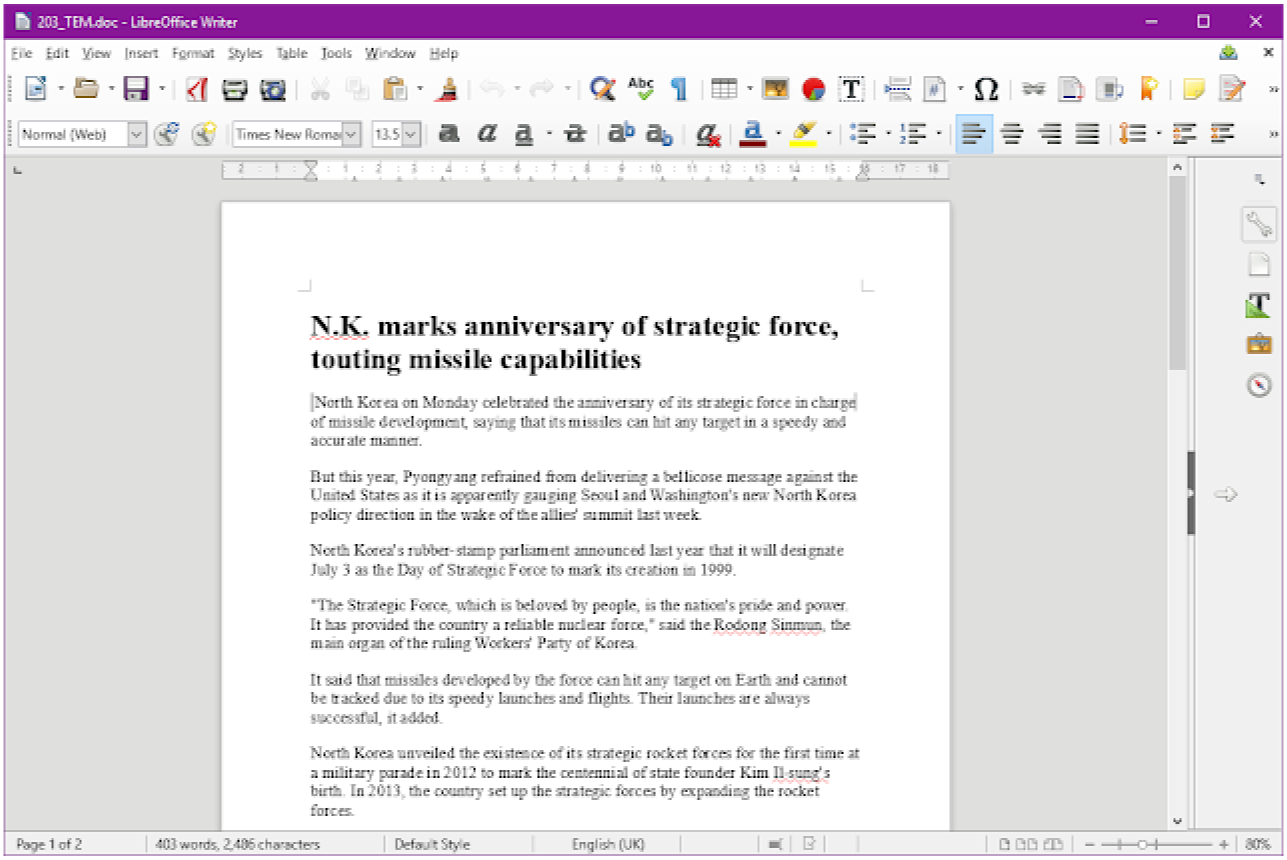
We recently wrote about the KONNI Remote Access Trojan (RAT) which has been distributed by a small number of campaigns over the past 3 years. We have identified a new distribution campaign which took place on 4th July. The malware used in this campaign has similar features to that distributed earlier in 2017 with the following changes:

- A new decoy document copy/pasted from an article published on the 3rd of July by Yonhap News Agency in Korea;
- The dropper includes a 64 bit version of KONNI;
- A new CC infrastructure consisting of a climbing club website.

North Korea conducted a test missile launch on 3rd July. This campaign appears to be directly related to the launch and the ensuing discussion of North Korean missile technology. This is consistent with previous KONNI distribution campaigns which have also frequently mentioned North Korea.

"N.K. marks anniversary of strategic force, touting missile capabilities" campaign

We identified an executable file, SHA-256 hash sum: 33f828ad462c414b149f14f16615ce25bd078630eee36ad953950e0da2e2cc90, which when opened displays the following Office document:


203_TEM.doc - LibreOffice Writer
File Edit View Insert Format Styles Table Tools Window Help
Normal (Web)
Times New Roman
13.5
Page 1 of 2
403 words, 2,486 characters
Default Style
English (UK)
80%

N.K. marks anniversary of strategic force, touting missile capabilities

North Korea on Monday celebrated the anniversary of its strategic force in charge of missile development, saying that its missiles can hit any target in a speedy and accurate manner.

But this year, Pyongyang refrained from delivering a bellicose message against the United States as it is apparently gauging Seoul and Washington's new North Korea policy direction in the wake of the allies' summit last week.

North Korea's rubber-stamp parliament announced last year that it will designate July 3 as the Day of Strategic Force to mark its creation in 1999.

"The Strategic Force, which is beloved by people, is the nation's pride and power. It has provided the country a reliable nuclear force," said the Rodong Sinmun, the main organ of the ruling Workers' Party of Korea.

It said that missiles developed by the force can hit any target on Earth and cannot be tracked due to its speedy launches and flights. Their launches are always successful, it added.

North Korea unveiled the existence of its strategic rocket forces for the first time at a military parade in 2012 to mark the centennial of state founder Kim Il-sung's birth. In 2013, the country set up the strategic forces by expanding the rocket forces.

The content of the document is a copy/pasted from an article published on July 3rd by Yonhap News Agency in Korea. In addition to displaying this document, the malicious executable also drops 2 different versions of KONNI:

```
C:\Users\Users\AppData\Local\MFAData\event\eventlog.dll (64 bit)
C:\Users\Users\AppData\Local\MFAData\event\errorevent.dll (32 bit)
```

On 64 bit versions of Windows, both files are dropped; on 32 bit versions of Windows, only errorevent.dll, the 32 bit version is dropped. Unlike previous campaigns, both binaries are packed with ASPack. In both cases, the dropped malware is immediately executed via rundll32.exe with one of the following registry keys created to ensure that the malware persists and is executed on rebooting the compromised system:

```
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\RTHDVCPE
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\RTHDVCP
```

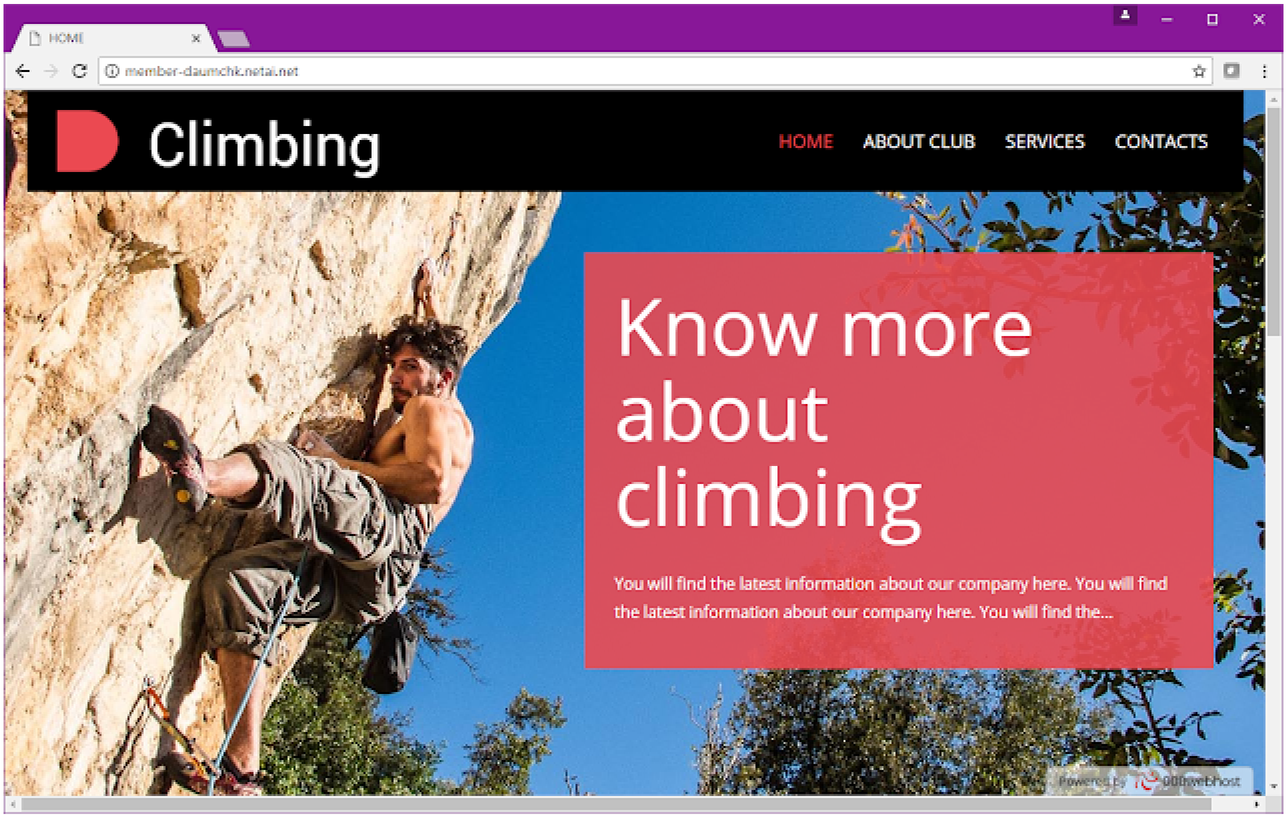
This attack uses a new Command & Control infrastructure hosted on the following domain:

member-daumchk[.]netai[.]net

The CnC traffic of KONNI takes place as HTTP post requests to web pages hosted as /weget/download.php, /weget/uploadtm.php or /weget/upload.php on the domain itself.

The attackers have gone to some effort to disguise the website as a legitimate climbing club.

Here is a screenshot of the website:

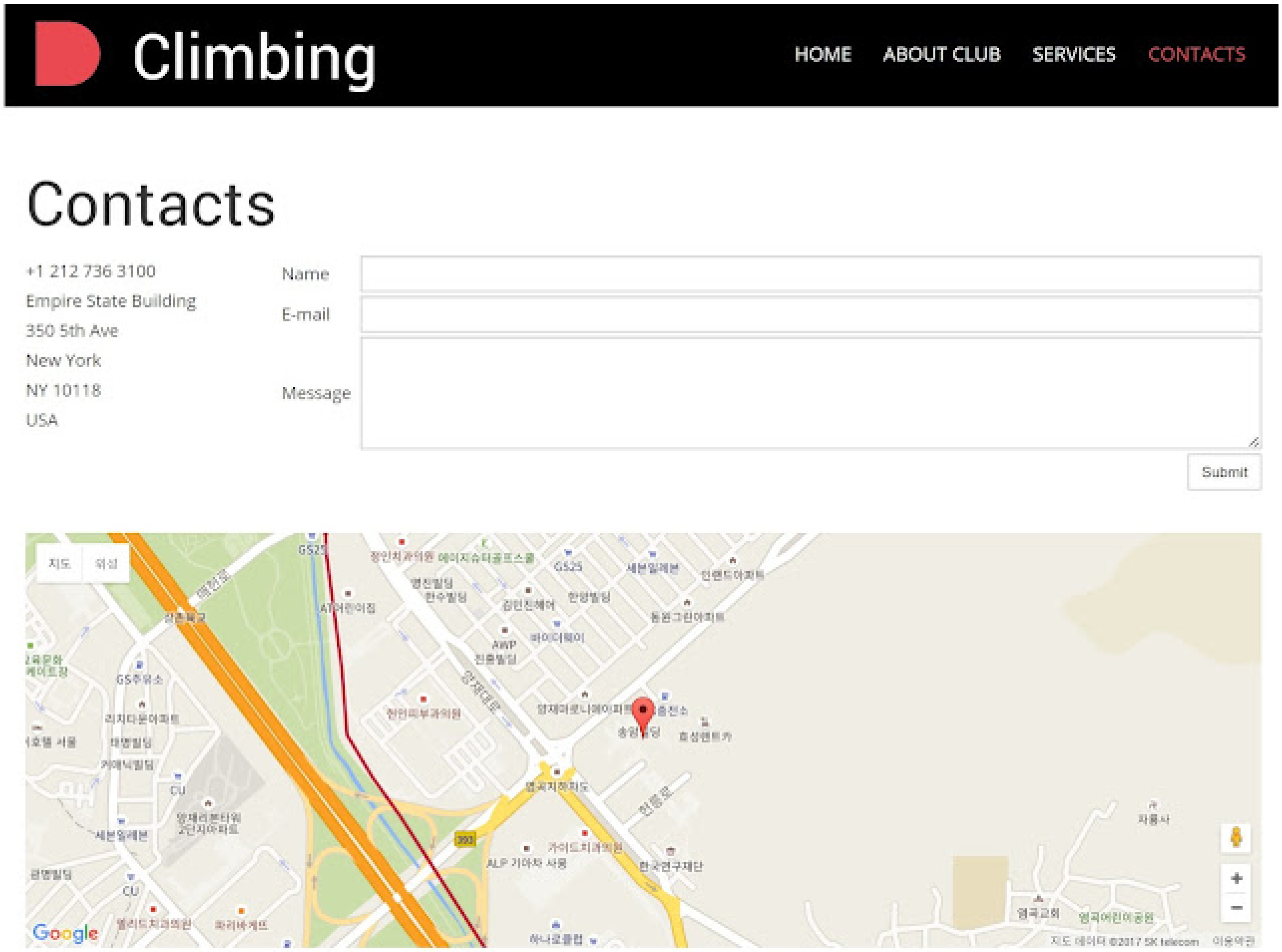


Know more about climbing

You will find the latest information about our company here. You will find the latest information about our company here. You will find the...

However, the website does not contain real text, only the default text of the Content Management System (CMS).

Additionally, the website contains a contacts section with an address in USA, but the map below the address is in Korean and points to a location in Seoul, South Korea:



Contacts

+1 212 736 3100
Empire State Building
350 5th Ave
New York
NY 10118
USA

Conclusion

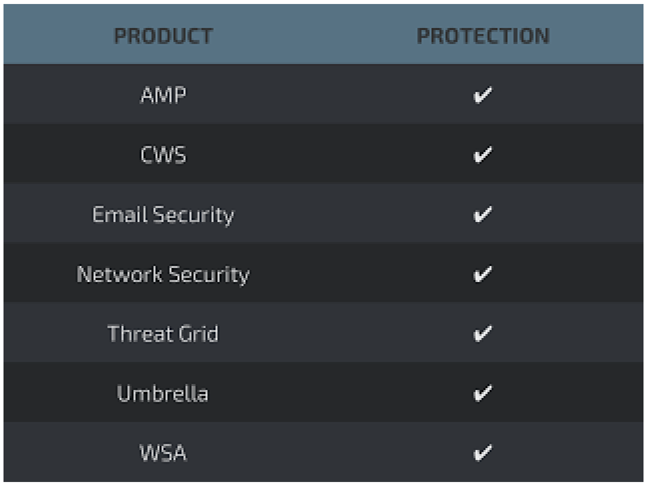
The KONNI malware distributed as part of this campaign is similar to previous versions that we have identified this year. The attackers have added a 64 bit version and used a packer to complicate analysis. This campaign is directly related to current events and is clearly 'fresh'. The binary was compiled on July 4th, the decoy document was published on July 3rd.

The threat actors associated with KONNI typically use decoy documents relating to North Korea, and this campaign is no exception. However, in contrast to the convincing decoy document lifted from a third party, the content of the decoy website hosted on the CnC server does not look legitimate. The text content is not consistent with the website navigation, and the contacts page contains a mis-match of a US address with a Korean map.

Nevertheless, this threat actor continues to remain active, and continues to develop updated versions of their malware. Organisations which may have an interest in the contents of this decoy document, and that used in previous campaigns should ensure that they are adequately protected against this and subsequent campaigns.

Coverage

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



PRODUCT	PROTECTION
AMP	✔
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.

CWS or 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.

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

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

IOC

File hashes

- Dropper: 33f828ad462c414b149f14f16615ce25bd078630eee36ad953950e0da2e2cc90
- 32 Bits binary: 290b1e2415f88fc3dd1d53db3ba90c4a760cf645526c8240af650751b1652b8a
- 64 bits binary: 8aef427aba54581f9c3dc923d8464a92b2d4e83cdf0fd6ace00e8035ee2936ad

Network

Member-daumchk[.]netai[.]net