2017 年 7 月 6 日，星期四

新 KONNI 攻击活动提及朝鲜导弹能力

作者：Paul Rascagneres

执行摘要

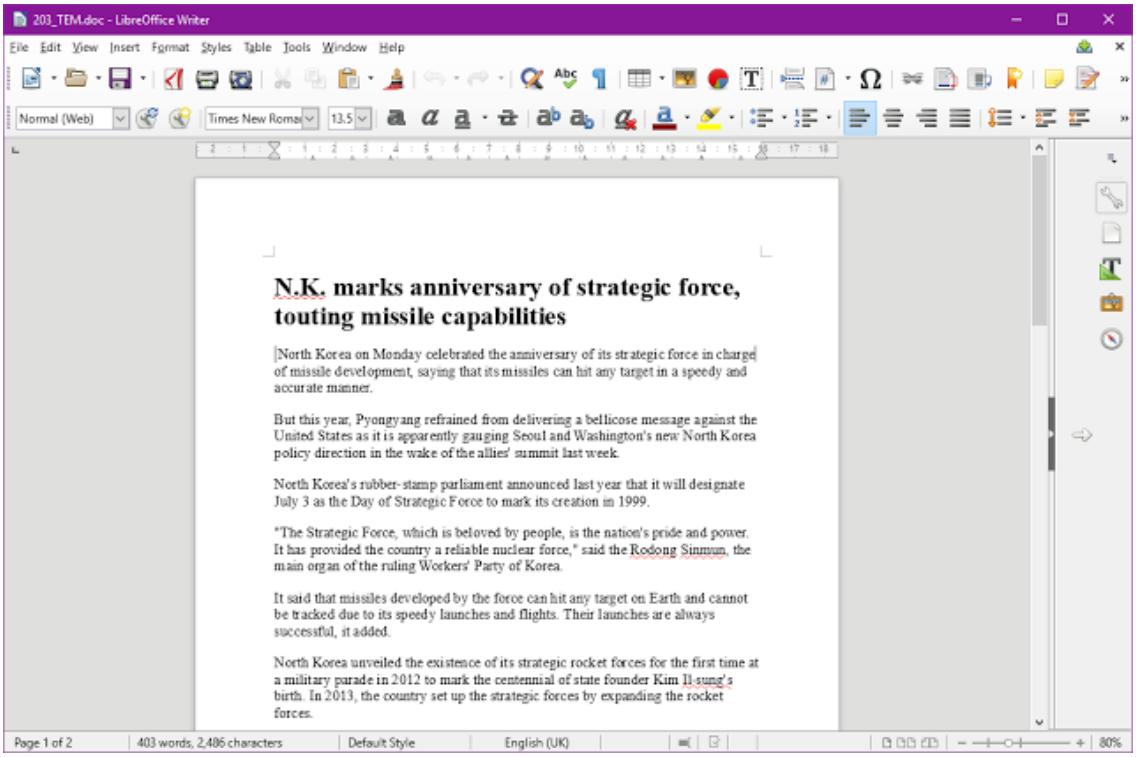
关于 3 年多以来仅出现在少数攻击活动中的 KONNI 远程访问木马 (RAT)，我们最近撰写过一篇文章。我们在 7 月 4 日发现，这种木马有新的分发活动。此次攻击活动中使用的恶意软件与 2017 年年初分发的恶意软件功能类似，但有以下变化：

- 新的诱饵文件复制/粘贴自韩国联合通讯社于 7 月 3 日发布的一篇文章；
- 植入程序包含 KONNI 的 64 位版本；
- 新的 CC 基础设施包含一个攀岩俱乐部网站。

朝鲜于 7 月 3 日进行了导弹发射试验。该攻击活动似乎与导弹发射和随后讨论的朝鲜导弹技术直接相关。这与之前同样频繁提及朝鲜的 KONNI 分发攻击活动一致。

“朝鲜庆祝战略导弹部队建军纪念日，展现导弹能力”攻击活动

通过研究此攻击活动，我们发现了一个可执行文件（SHA-256 散列和：33f828ad462c414b149f14f16615ce25bd078630eee36ad953950e0da2e2cc90），打开该文件会显示以下 Office 文档：



该文档的内容来自韩国联合通讯社 7 月 3 日发布的一篇文章。除了显示本文档之外，该恶意可执行文件还会植入两个不同版本的 KONNI：

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

在 Windows 64 位版本中，该恶意可执行文件会同时植入这两个文件；而在 Windows 32 位版本中，该恶意可执行文件只会植入 32 位版本 errorevent.dll。与早先的攻击活动不同的是，这两个二进制文件通过 ASPack 打包。无论是在哪种 Windows 64 版本中，植入的恶意软件都会立即通过 rundll32.exe 执行，并创建以下任一注册表项来确保恶意软件的持久性，并在被感染系统重新启动时执行：

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

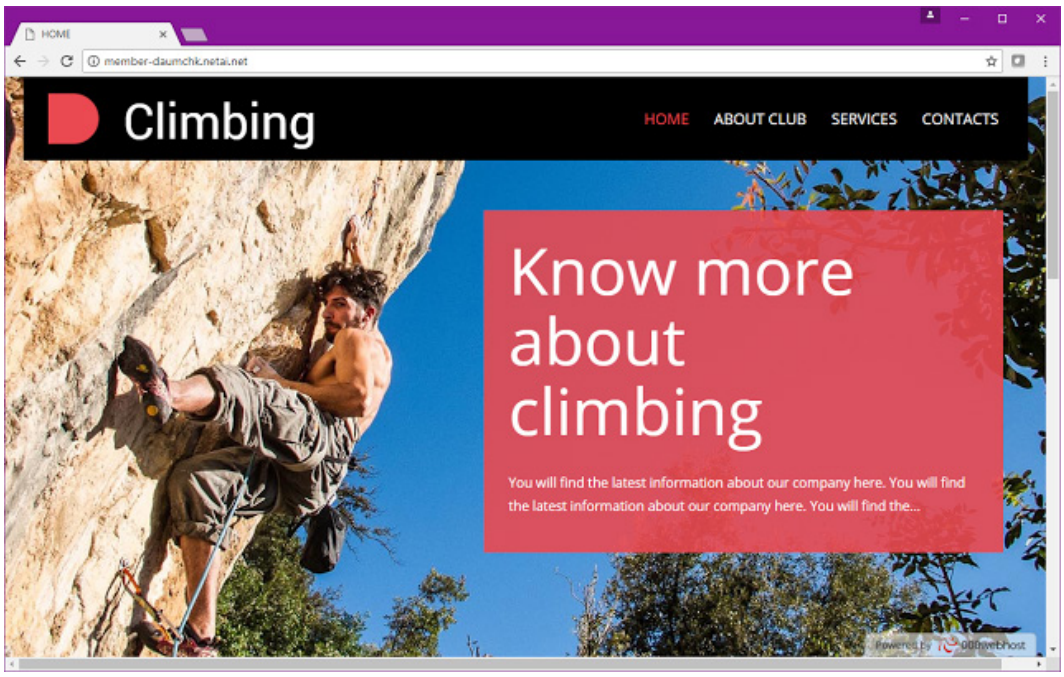
此攻击使用以下域中托管的新“命令和控制”基础设施：

- member-daumchk[.]netai[.]net

当 HTTP 向域中托管的 /weget/download.php、/weget/uploadtm.php 或 /weget/upload.php 网页发送请求时，KONNI 会产生 CnC 流量。

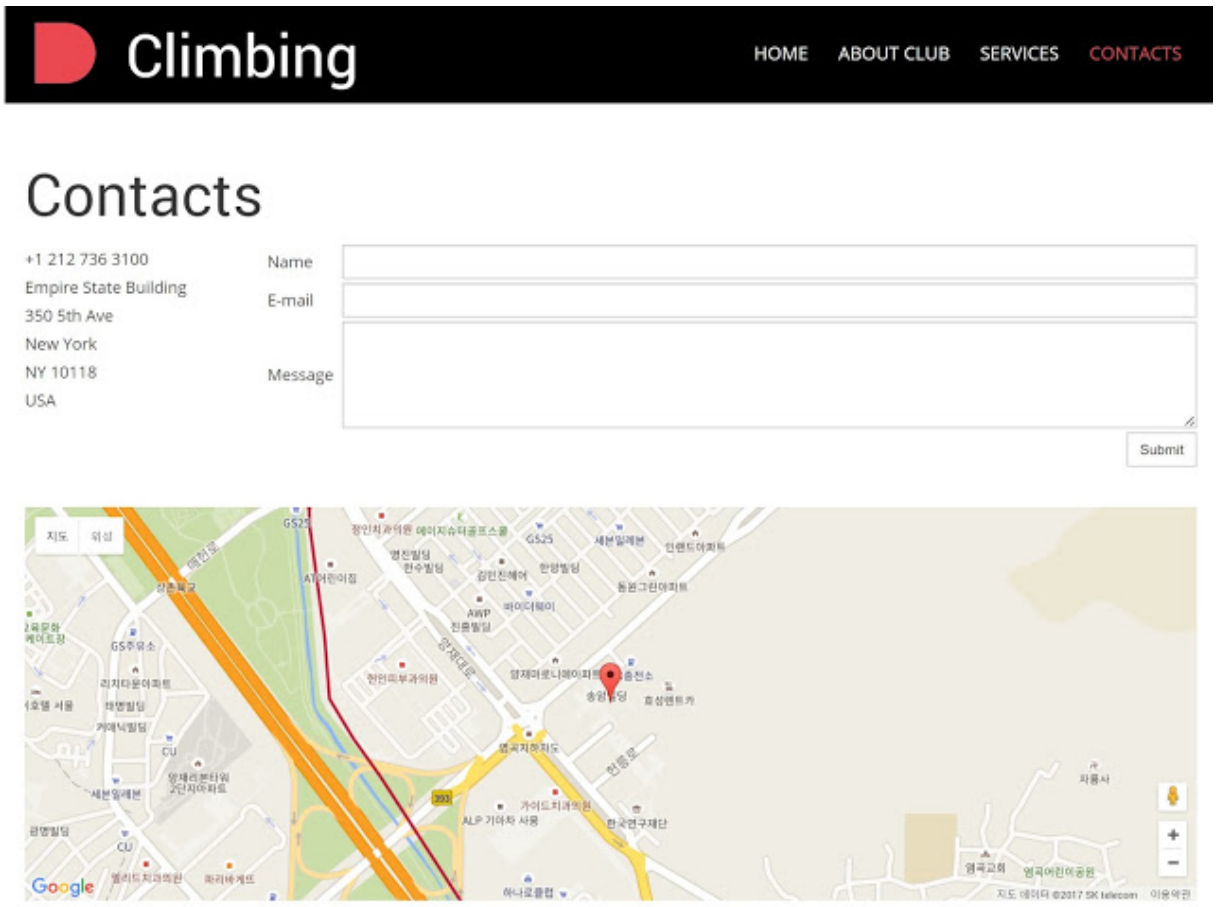
攻击者已设法将该网站伪装成合法的攀岩俱乐部网站。

以下是该网站的屏幕截图：



但是，这个网站上不包含任何实际文本，只有内容管理系统 (CMS) 的默认文本。

此外，虽然该网站“联系信息”部分显示的联系地址是在美国，但地址下方的地图却指向韩国首尔的某个位置：



结论

在该攻击活动中分发的 KONNI 恶意软件与我们今年早先发现的版本类似。攻击者只是添加了一个 64 位版本并使用打包程序让分析变得更加复杂。这次攻击活动与时事直接相关，而且明显是“新鲜出炉”的内容。二进制文件是在 7 月 4 日编译的，诱饵文件是在 7 月 3 日发布的。

与 KONNI 相关的威胁发起者通常使用与朝鲜有关的诱饵文档，这次攻击活动也不例外。但是，对比来自第三方的可信服诱饵文档，这个托管在 CnC 服务器上的诱饵网站的内容看起来并不合法：文本内容与网站导航不一致，并且“联系信息”页面包含的美国地址与韩国地图不匹配。

尽管如此，威胁发起者仍继续保持活跃，并不断开发这款恶意软件的升级版本。如果对此诱饵文件的内容以及之前的攻击活动中使用的内容感兴趣，组织应当采取切实保护措施来防御此攻击活动以及后续攻击活动。

防护

思科客户可通过其他方式检测并阻止此威胁，包括：

产品	保护
AMP	✔
CWS	✔
邮件安全	✔
网络安全	✔
Threat Grid	✔
Umbrella	✔
WSA	✔

高级恶意软件防护 (AMP) 解决方案可以有效防止执行威胁发起者使用的恶意软件。

CWS 或 WSA 的 Web 扫描功能可以阻止访问恶意网站，并检测这些攻击中所用的恶意软件。

邮件安全设备可以拦截威胁发起者在攻击活动中发出的恶意邮件。

IPS 和 NGFW 的网络安全防护功能拥有最新的签名库，可以检测威胁发起者的恶意网络活动。

AMP Threat Grid 可帮助识别恶意二进制文件，使所有思科安全产品都有内置保护措施。

Umbrella，我们的安全互联网网关 (SIG)，可阻止用户连接恶意域、IP 和 URL（无论用户是否位于公司网络上）

IOC

文件散列值

- 植入程序：33f828ad462c414b149f14f16615ce25bd078630eee36ad953950e0da2e2cc90
- 32 位二进制文件：290b1e2415f88fc3dd1d53db3ba90c4a760cf645526c8240af650751b1652b8a
- 64 位二进制文件：8aef427aba54581f9c3dc923d8464a92b2d4e83cdf0fd6ace00e8035ee2936ad

网络

- Member-daumchk[.]netai[.]net

发布者：PAUL RASCAGNERES；发布时间：3:58
标签：APT、KONNI、朝鲜、恶意软件、恶意软件分析、RAT