New Defray Ransomware Targets Education and Healthcare Verticals

proofpoint.com/us/threat-insight/post/defray-new-ransomware-targeting-education-and-healthcare-verticals

August 24, 2017

Blog
Threat Insight
New Defray Ransomware Targets Education and Healthcare Verticals

August 24, 2017 Proofpoint Staff

Defray Ransomware Overview

Proofpoint threat researchers recently analyzed Defray Ransomware, a previously undocumented ransomware strain. So far in August, we have observed only two small and selectively targeted attacks distributing this ransomware. One was primarily aimed at Healthcare and Education verticals; another targeted Manufacturing and Technology verticals. We selected the name “Defray” based on the command and control (C&C) server hostname from the first observed attack:

defrayable-listings[.]000webhostapp[.]com

Coincidentally, the verb *defray* means to provide money to pay a portion of a cost or expense, although what victims are defraying in this case is unclear.

Defray Malware Distribution

The distribution of Defray malware has several notable characteristics:

- Defray is currently being spread via Microsoft Word document attachments in email
- The campaigns are as small as several messages each
- The lures are custom crafted to appeal to the intended set of potential victims
- The recipients are individuals or distribution lists, e.g., group@ and websupport@
- Geographic targeting is in the UK and US
- Vertical targeting varies by campaign and is narrow and selective

On August 22, Proofpoint researchers detected an email campaign targeted primarily at Healthcare and Education involving messages with a Microsoft Word document containing an embedded executable (specifically, an OLE packager shell object). In the screenshot shown in Figure 1, the attachment uses a UK hospital logo in the upper right (not shown) and purports to be from the Director of Information Management & Technology at the hospital.

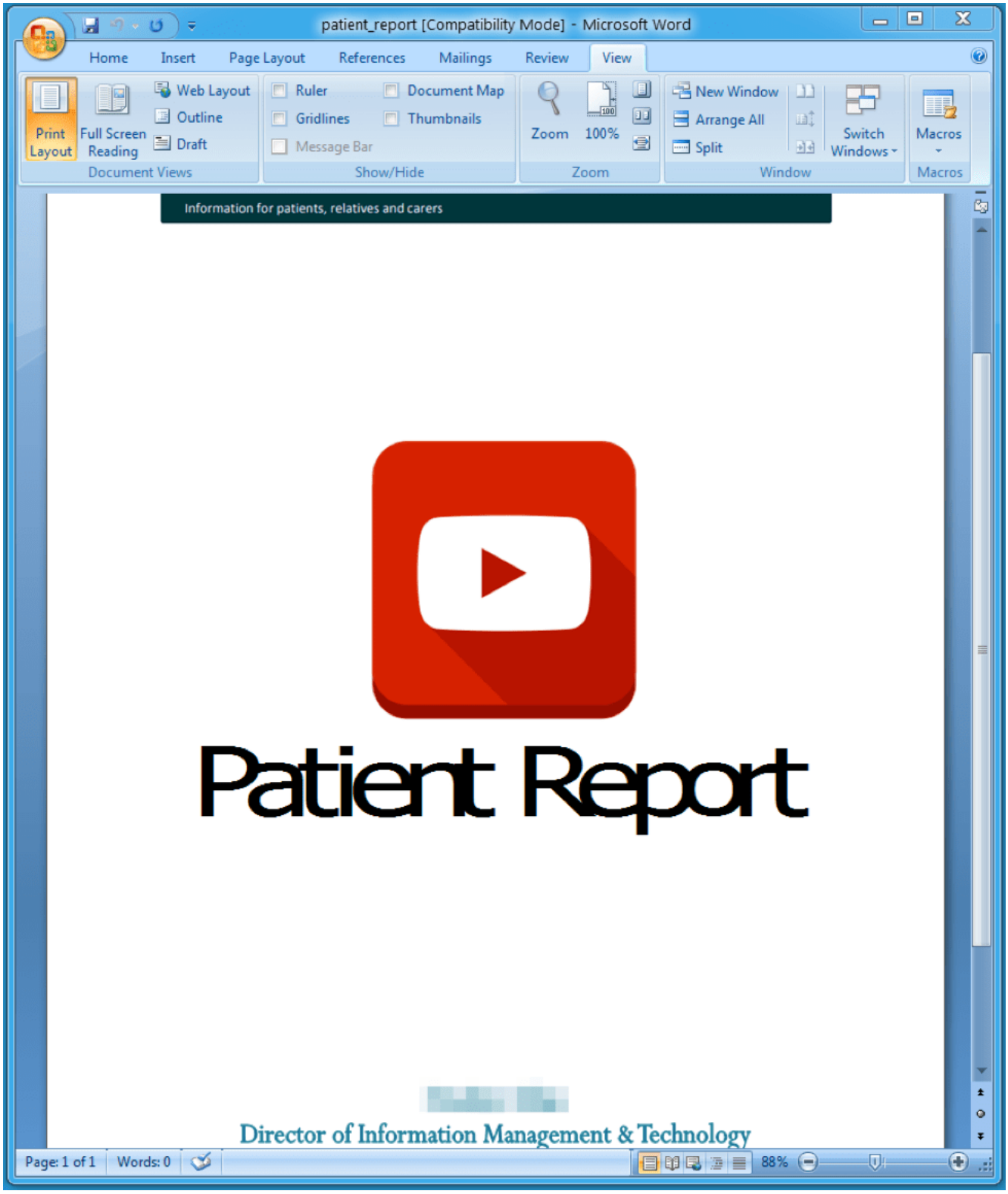

Figure 1: The Word document, patient_report.doc, delivered in malicious email messages

This was similar to a campaign observed by Proofpoint researchers on August 15 targeting Manufacturing and Technology verticals and involving messages with the subject “Order/Quote” and a Microsoft Word document containing an embedded executable (also an OLE packager shell object).

In the August 15 campaign, the attachment used a lure referencing a UK-based aquarium with international locations (Figure 2), and purported to be from a representative of the aquarium.

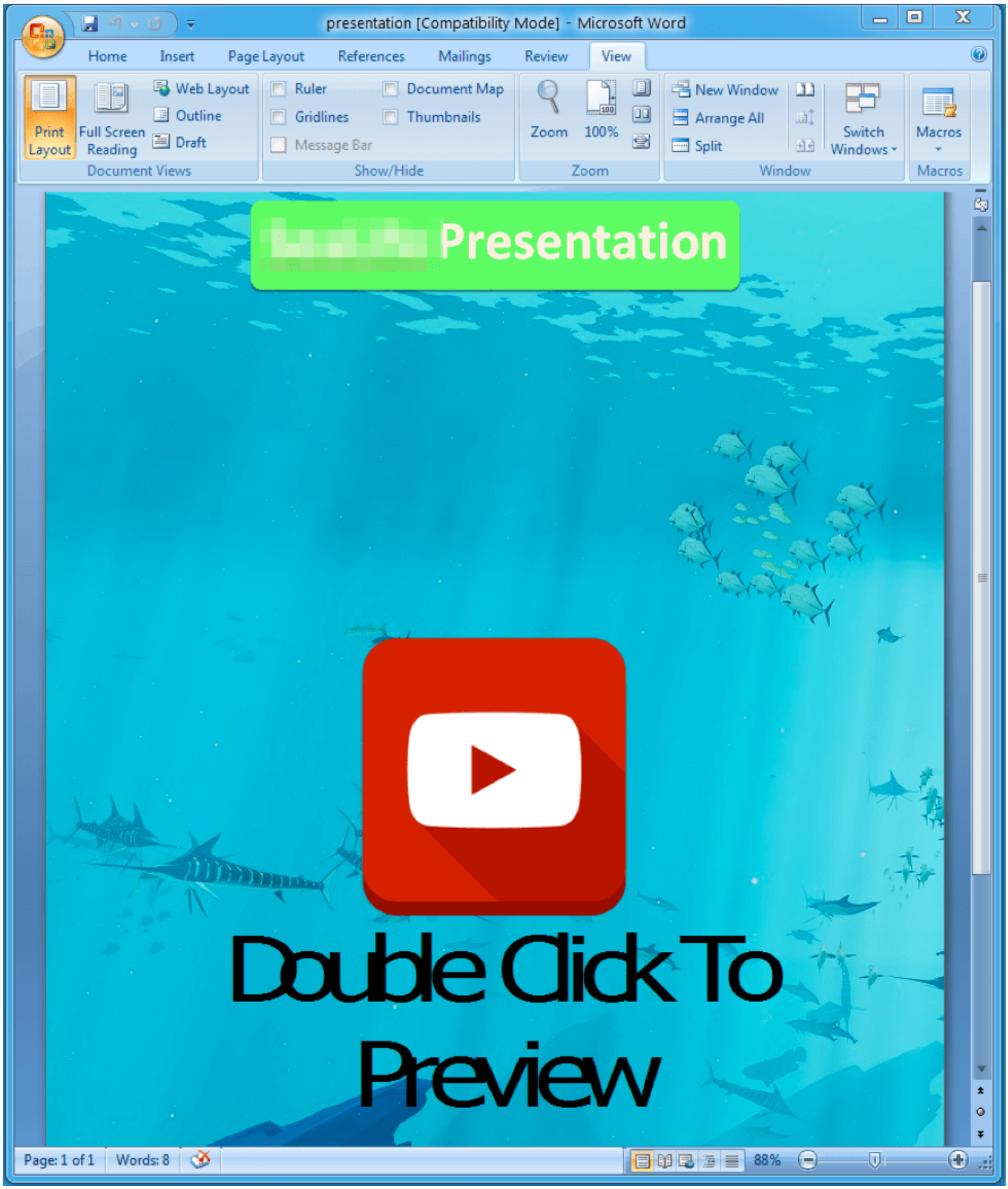

Figure 2: Word document attachment, presentation.doc, delivered in malicious email messages

If the potential victim double clicks on the embedded executable, the ransomware is dropped with a name such as taskmgr.exe or explorer.exe in the %TMP% folder and executed.

Defray Analysis

To alert the victim that their computer has been infected and that their files are encrypted, this ransomware creates FILES.TXT (Figure 3) in many folders throughout the system. HELP.txt, with identical content to FILES.txt, also appeared on the Desktop folder where we executed the ransomware.

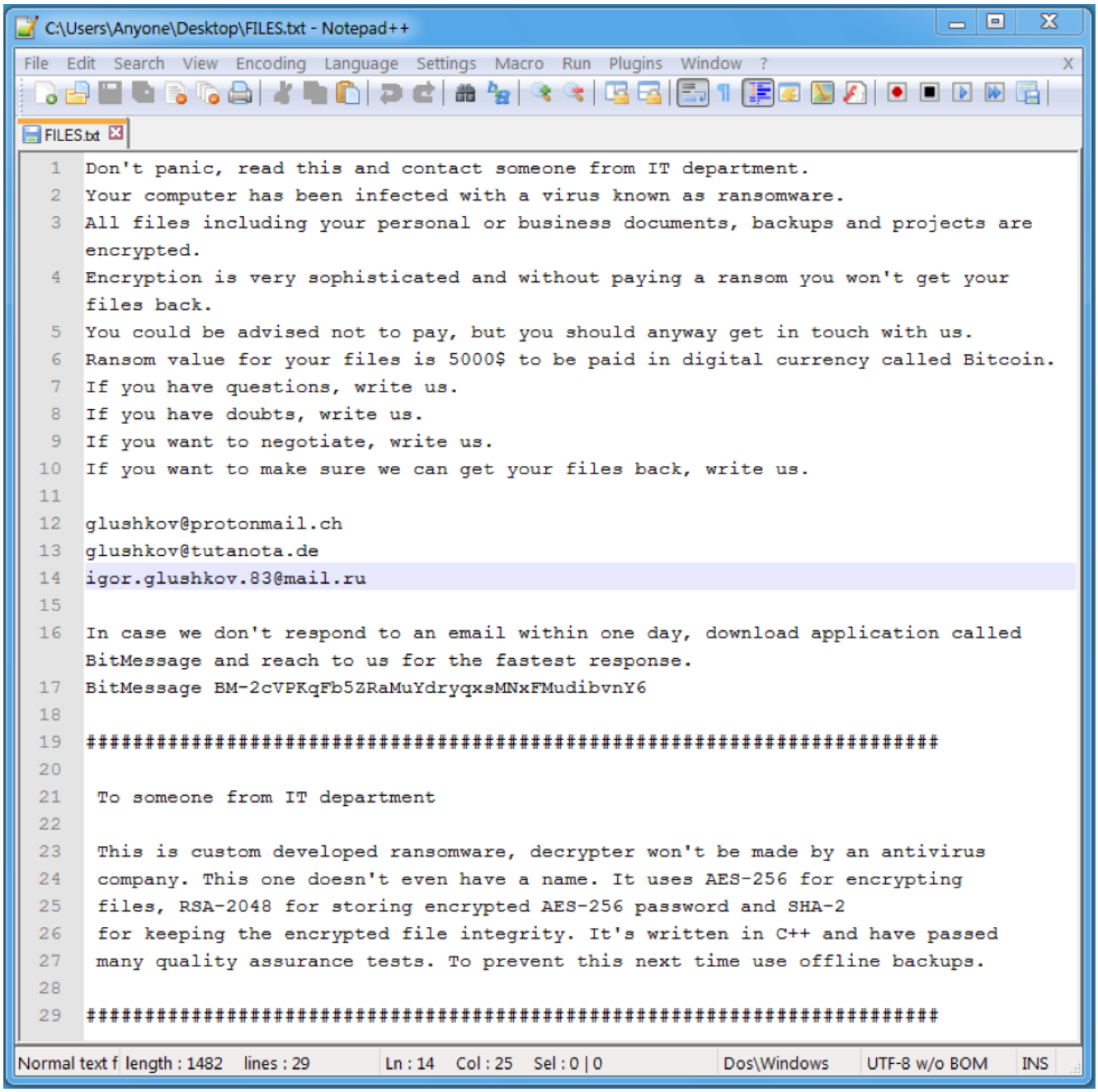

Figure 3: FILES.txt ransom message

The ransom note shown in Figure 3 follows a recent trend of fairly high ransom demands; in this case, $5000. However, the actors do provide email addresses so that victims can potentially negotiate a smaller ransom or ask questions, and even go so far as to recommend BitMessage as an alternative for receiving more timely responses. At the same time, they also recommend that organizations maintain offline backups to prevent future infections.

The ransomware contains a hardcoded list of file extensions, shown below, for files that it will encrypt (although we observed others such as .lnk and .exe encrypted that were not on this list). The file extensions of modified files were not changed. We observed that the modified files all end in bytes “30 82 04 A4 02 01 00 02 82 01 01 00 9F CF 52 84” for our sample. We did not investigate the specifics of the encryption routine.

.001 | .3ds | .7zip | .MDF | .NRG | .PBF | .SQLITE | .SQLITE2 | .SQLITE3 | .SQLITEDB | .SVG | .UIF | .WMF | .abr | .accdb | .afi | .arw | .asm | .bkf | .c4d | .cab | .cbm | .cbu | .class | .cls | .cpp | .cr2 | .crw | .csh | .csv | .dat | .dbx | .dcr | .dgn | .djvu | .dng | .doc | .docm | .docx | .dwfx | .dwg | .dxf | .fla | .fpx | .gdb | .gho | .ghs | .hdd | .html | .iso | .iv2i | .java | .key | .lcf | .matlab | .max | .mdb | .mdi | .mrbak | .mrimg | .mrw | .nef | .odg | .ofx | .orf | .ova | .ovf | .pbd | .pcd | .pdf | .php | .pps | .ppsx | .ppt | .pptx | .pqi | .prn | .psb | .psd | .pst | .ptx | .pvm | .pzl | .qfx | .qif | .r00 | .raf | .rar | .raw | .reg | .rw2 | .s3db | .skp | .spf | .spi | .sql | .sqlite-journal | .stl | .sup | .swift | .tib | .txf | .u3d | .v2i | .vcd | .vcf | .vdi | .vhd | .vmdk | .vmem | .vmwarevm | .vmx | .vsdx | .wallet | .win | .xls | .xlsm | .xlsx | .zip

Defray has been observed communicating with an external C&C server via both HTTP (clear-text, shown in Figure 4) and HTTPS, to which it will report infection information.

Figure 4: Screenshot of the clear-text C&C beacon

After encryption is complete, Defray may cause other general havoc on the system by disabling startup recovery and deleting volume shadow copies. On Windows 7 the ransomware monitors and kills running programs with a GUI, such as the task manager and browsers. We have not observed the same behavior on Windows XP.

Conclusion

Defray Ransomware is somewhat unusual in its use in small, targeted attacks. Although we are beginning to see a trend of more frequent targeting in ransomware attacks, it still remains less common than large-scale “spray and pray” campaigns. It is also likely that Defray is not for sale, either as a service or as a licensed application like many ransomware strains. Instead, it appears that Defray may be for the personal use of specific threat actors, making its continued distribution in small, targeted attacks more likely. We will continue to monitor this threat and provide updates as new information emerges.

Defray Ransomware Indicators of Compromise (IOCs)

IOC	IOC Type	Description
947b360b76dd815f5b5d226b8a9aba22fe6b5589a3c16c765625ce2f9d1f5db2	sha256	Defray binary
defrayable-listings.000webhostapp[.]com	dns	C&C Domain
145.14.145[.]115	ip	C&C IP
kinaesthetic-electr.000webhostapp[.]com	dns	C&C Domain
08cf8ed94cc1ef6ae23133f3e506a50d8aad9047c6fa74568a0373d991261aa4	sha256	Defray binary

ET and ETPRO Suricata/Snort Signatures

2827545 ETPRO TROJAN W32.Defray Ransomware Checkin

2827635 ETPRO TROJAN Observed Malicious Domain SSL Cert in SNI (Defray Ransomware)

Subscribe to the Proofpoint Blog