Iron Tiger Compromises Chat Application Mimi, Targets Windows, Mac, and Linux Users

SHA256
56b55e3587dc8e40e36c2eadba62dd2b39890dc0df313620f3b42ab0f0b92a3d HyperBro DLL (Windows) Trojan.Win32.HYPERBRO.AF
22c3c2bf77a94ed5f207c00e240f558d6411308d237779ffb12e04bbe2c90356 HyperBro DLL (Windows) TROJ_FRS.VSNTGC22
ef2f20d1016cd39ff44f1399c8aa5c1ff5bfd4850d611ba375fbeff7f7e3eaf6 HyperBro packed payload (Windows) Trojan.Win32.HYPERBRO.AE
d0fec5c5e2687e76af07a4a3c6e2e2b02789838c0b802f5041443ab482bc3498 Rshell (Linux) Trojan.Linux.RSHELL.A
07aa739fa4942cfd68d4a075568456797f11ae34db5cd56f88d80185bc1d7a29 Rshell (Linux) Trojan.Linux.RSHELL.A
d67aebfafa347a21805dbded3fa310e2268a5d2255fcb7f1c8004502a95e7538 Rshell (Linux) Trojan.Linux.RSHELL.A
e909c4dac832e9d1ecd1673c5bff6e1939d9c832a2509cb64931e4aa1e334077 Rshell (Linux) Trojan.Linux.RSHELL.A
c10a3a78cdf1e48189ac270767f7f718bd15a9d4e48e580a9ef6ceff5f4abf46 Rshell (Linux) Trojan.Linux.RSHELL.A
8019b7deaf41b48c38b8b48e016f208a28e0909d437d4e35e3e35f7995758564 Rshell (Linux) Trojan.Linux.RSHELL.A
3a9e72b3810b320fa6826a1273732fee7a8e2b2e5c0fd95b8c36bbab970e830a Rshell (Mac OS) Backdoor.MacOS.REVSHELL.MANP
8c3be245cbbe9206a5d146017c14b8f965ab7045268033d70811d5bcc4b796ec Rshell (Mac OS) Backdoor.MacOS.REVSHELL.MANP

URLs
time.ntp-server.asia C&C
45.142.214.193 C&C
linux.updatelive-oline.com C&C
center.veryssl.org C&C
https://139.180.216.65:443/api/v2/ajax C&C
https://104.168.211.246:443/api/v2/ajax C&C
https://80.92.206.158:443/api/v2/ajax C&C
https://45.77.250.141:443/api/v2/ajax C&C
http://139.180.216.65/dlpprem32.dll Disease Vector
http://139.180.216.65/dlpprem32.bin Disease Vector

http://139.180.216.65/rshell Disease Vector
http://45.77.250.141/dlpprem32.dll Disease Vector
http://45.77.250.141/dlpprem32.bin Disease Vector