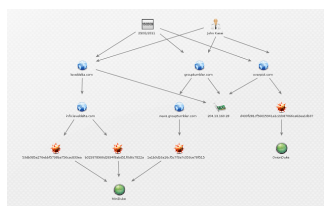
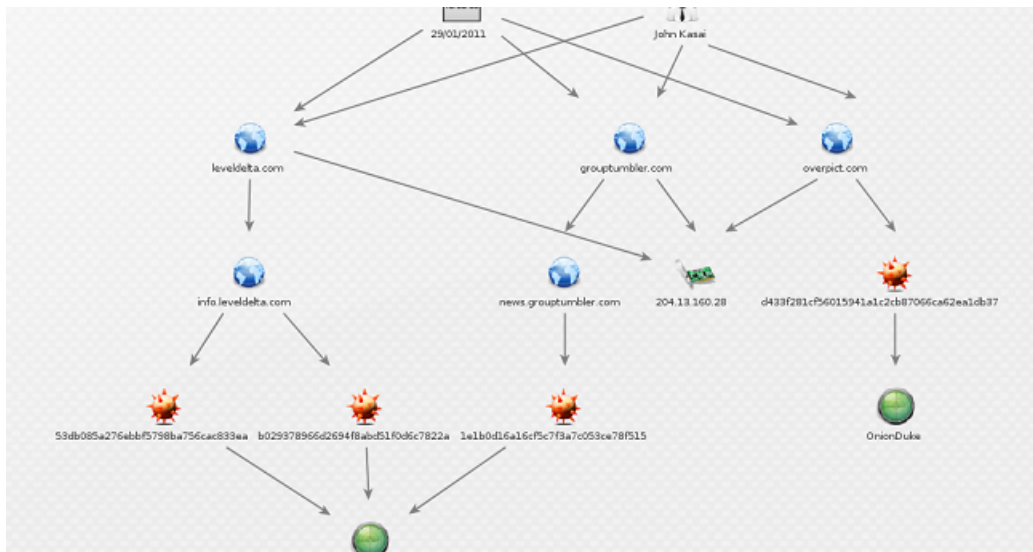


OnionDuke samples

contagiodump.blogspot.com/2014/11/onionduke-samples.html



Research: F-Secure: OrionDuke: APT Attacks Via the Tor Network

Download



[Download. Email me if you need the password \(new link\)](#)

File attributes

Size: 219136

MD5: 28F96A57FA5FF663926E9BAD51A1D0CB

Size: 126464

MD5: C8EB6040FD02D77660D19057A38FF769

Size: 316928

MD5: D1CE79089578DA2D41F1AD901F7B1014

Virustotal info

<https://www.virustotal.com/en/file/366affd094cc63e2c19c5d57a6866b487889dab5d1b07c084fff94262d8a390b/analysis/>

SHA256: 366affd094cc63e2c19c5d57a6866b487889dab5d1b07c084fff94262d8a390b

File name: 366affd094cc63e2c19c5d57a6866b487889dab5d1b07c084fff94262d8a390b

Detection ratio: 8 / 52

Analysis date: 2014-11-15 18:37:30 UTC (8 hours, 44 minutes ago)

Antivirus Result Update

Baidu-International Trojan.Win32.Agent.adYf 20141107

F-Secure Backdoor:W32/OnionDuke.B 20141115
Ikarus Trojan.Win32.Agent 20141115
Kaspersky Backdoor.Win32.MiniDuke.x 20141115
Norman OnionDuke.A 20141115
Sophos Troj/Ransom-ALA 20141115
Symantec Backdoor.Miniduke!gen4 20141115
Tencent Win32.Trojan.Agent.Tbsl 20141115

<https://www.virustotal.com/en/file/366affd094cc63e2c19c5d57a6866b487889dab5d1b07c084fff94262d8a390b/analysis/>

SHA256: 366affd094cc63e2c19c5d57a6866b487889dab5d1b07c084fff94262d8a390b
File name: 366affd094cc63e2c19c5d57a6866b487889dab5d1b07c084fff94262d8a390b
Detection ratio: 8 / 52
Antivirus Result Update

Baidu-International Trojan.Win32.Agent.adYf 20141107
F-Secure Backdoor:W32/OnionDuke.B 20141115
Ikarus Trojan.Win32.Agent 20141115
Kaspersky Backdoor.Win32.MiniDuke.x 20141115
Norman OnionDuke.A 20141115
Sophos Troj/Ransom-ALA 20141115
Symantec Backdoor.Miniduke!gen4 20141115
Tencent Win32.Trojan.Agent.Tbsl 20141115

<https://www.virustotal.com/en/file/0102777ec0357655c4313419be3a15c4ca17c4f9cb4a440bfb16195239905ade/analysis/>

SHA256: 0102777ec0357655c4313419be3a15c4ca17c4f9cb4a440bfb16195239905ade
File name: 0102777ec0357655c4313419be3a15c4ca17c4f9cb4a440bfb16195239905ade
Detection ratio: 19 / 55
Analysis date: 2014-11-15 18:37:25 UTC (8 hours, 47 minutes ago)
Antivirus Result Update

AVware Trojan.Win32.Generic!BT 20141115
Ad-Aware Backdoor.Generic.933739 20141115
Baidu-International Trojan.Win32.OnionDuke.BA 20141107
BitDefender Backdoor.Generic.933739 20141115
ESET-NOD32 a variant of Win32/OnionDuke.A 20141115
Emsisoft Backdoor.Generic.933739 (B) 20141115
F-Secure Backdoor:W32/OnionDuke.A 20141115
GData Backdoor.Generic.933739 20141115
Ikarus Trojan.Win32.Onionduke 20141115
Kaspersky Backdoor.Win32.MiniDuke.x 20141115
McAfee RDN/Generic BackDoor!zw 20141115
McAfee-GW-Edition BehavesLike.Win32.Trojan.fh 20141114
MicroWorld-eScan Backdoor.Generic.933739 20141115
Norman OnionDuke.B 20141115
Sophos Troj/Ransom-ANU 20141115
Symantec Backdoor.Miniduke!gen4 20141115
TrendMicro BKDR_ONIONDUKE.AD 20141115
TrendMicro-HouseCall BKDR_ONIONDUKE.AD 20141115
VIPRE Trojan.Win32.Generic!BT 20141115