




# ORANGEWORM



## ORANGEWORM

 -  US , EUROPE , ASIA  BACKDOORS



---

# A SURVEY ON ORANGEWORM ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

## - NERDS OF AXIAL

### I. INTRODUCTION

Orangeworm is a threat group which is believed to be based of a corporate espionage .

\*Orangeworm has been linked tto attacks on healthcare sector on various nations.

FBI investigators said the group has been active since 2016 when the first attacks with the Kwampirs remote access trojan (RAT) have been observed in the wild.

### IV. CAMPAIGNS

### II. TARGETS

Hospitality , agriculture, healthcare IT service providers, pharmaceutical manufacturers, and healthcare equipment producers.

### ATTRIBUTION

### III. METHODS USED

Orangeworm installs Trojan.Kwampirs the Trojan decrypts and extracts a copy of its primary DLL payload – which comes from itsresource area. The Becker’s summary also notes the injection of the randomly generated characters within the decrypted payload, with which it is able to sidestep hash-based detection systems

The researchers who released this most recent report suggest that this healthcare attack is probably not sponsored by North Korea or another foreign government; instead, it is believed to be a team of individuals. It is not possible, in terms of what can be gathered about the way the Orangeworm group is acting or by the technical nature of its attacks, tofigure out the nation from which the attacks arebeing launched.

[cited from Symantec]

Once Kwampirs is on a computer, the hackers are able to make the malware’s toolset more robust. They can download and run other modules within memory if that is what the attacker wants to do. The additional modules allow the criminal to customize their efforts to the environment of their target so that it is possible for them to accomplish what they want, which is broad information theft.



## V. IOCS

---

### Hashes

07f5fa96d31ed75edba8699f53a75502ade214b34469163011ced5b94e393f32  
12c6c48e1e52ebca20f4b890922fb31965317865d35ac04d216ad8b78f866999  
1486746bdba1161cfc15f37011c815911c33a2abd657198b835ac5f8eede663c  
281c2ad26346305dac90ce33c2c417b6a7271f990ba9fa5c7db65d6f2e501e94  
2d801f75a52f65ffb053ae052cad45a919afd431f5ca46e86abe3d9274c903e4  
2f04f6b04a735d4ccbc196942acbd3f7a64bc588a0107fc9e344df62a41ad85d  
303379ebb41bcb39bc8c5b7c102cff1a90a2ee207a51e0c0fd83c0348ea436a5  
34ce48c7481118aac4b5d772a64e0edf8e107a7f606913c49493d5dbc06f96d7  
39f8dd73baa0dd67607784b40fb4ad5881b50bb69a59eee2a844b615753062ed  
3b3c9a372188fea46b05e9253e03473fda963aaa76fdd459590ecca9db5af9fb  
3d0dbd119e9f1dd57db3331834c5206c4df321f3f6799c9a622f1a8abe462b2d  
64defebf7e600d92685672c4b4d3d2ed3fc6cca27663a65c42df61843573297b  
75d93cd55d54a38a9ec47efe26f4a2c4c8c14328175fdd8d69efc0187cef6a2e  
768fab04b19c18e375183bd762eda75359da3a964aa97000639cdfdd066f6edd  
7f9531e47146095f681564cfd5d322af3def6468202f62c6215af29c0453fb0a  
83a0b4476a0f50321308e4e1b4d680430e29a53b9669174d8113d6dcbca817e2  
85f8fa27a5f013d38a3c4a3742fbc43df90196326110fda9ad05ac2366d3e525  
908d608f2b39b37a2a72cbdd96476acc1159341927d41103370432ddf148b4d9  
97dd250670cef14e04db0145efe7fcfc945018b681e87e48a6f012fd7f79d02e  
a2d2584e1c46bc2954aaf47957f7fb48bc8209cdf04c1ccd226d689094a2b761  
b489e5469938f1410a955ab26dc2cb2c81923c75f545df3c351767d5f13b728d  
b570b07b43cdef3fe2f636a9db6da3dd1e2cb68d980a5fe5b3225713d4ce3e8f  
c783f6180147abfa55e8c6dc137b506b595ea111589a1ba4a870778b1f309b8c  
cade857aa5735467a69af2267f6c6179286bd5d1ad61b60332a21527b69d9736  
ced9a61ebaa8de7aa360ad2d24be26e2474fa4164118f8e32f4e2b2aba6ce511  
d1953d2c07d0572063364f34de99950407d07bd376dd9817ac799d5628ae5339  
d881198d26d10fc3a3ace876d4ef0db373b586de28a8b489248f3ea1840ba683  
e3bc08f7a12f9b68a73de99ecd0aaef1447bbba9e35f518d42fd0e751be858f  
f8eb3a2054d6bc51fc0a127f9c01c4aaf238c0c681c36164a716268dc452ff91

## VI. REFERENCES

<https://www.zdnet.com/article/fbi-re-sends-alert-about-supply-chain-attacks-for-the-third-time-in-three-months/>

<https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Orangeworm>

<https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia>

<https://www.securityartwork.es/2019/03/13/orangeworm-group-kwampirs-analysis-update/>

