

Ozone RAT Now Leveraged In the Wild

Priority Intelligence Report

Publication date: 9 December 2015

Handling requirements: Traffic light protocol (TLP) WHITE. TLP WHITE information may be distributed without restriction, subject to copyright controls.

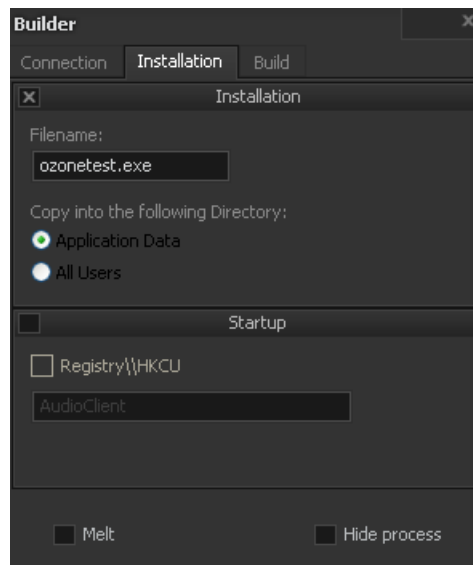
Details

In late November 2015, Wapack Labs observed a targeted spear phishing attack that leveraged an unidentified malware variant. The malware was subsequently identified as the Ozone Remote Administration Tool (RAT). Ozone is just the latest in the line of commercially available tools which are increasing in popularity due to their convenience, affordability and robust capabilities.




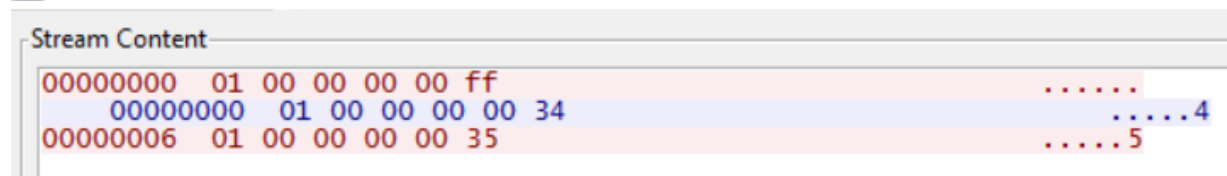
Ozone was first released for sale on 8 September 2015 and is currently marketed on ozonercp.com. The tool is offered in both a Standard (\$20) and Platinum package (\$50). The Platinum package comes with additional tools for Crypto mining as well as weaponizing the payload into a malicious macro. The builder and controller are similar in functionality to other RATs on the market. Connection and installation features are easily configurable by the user.





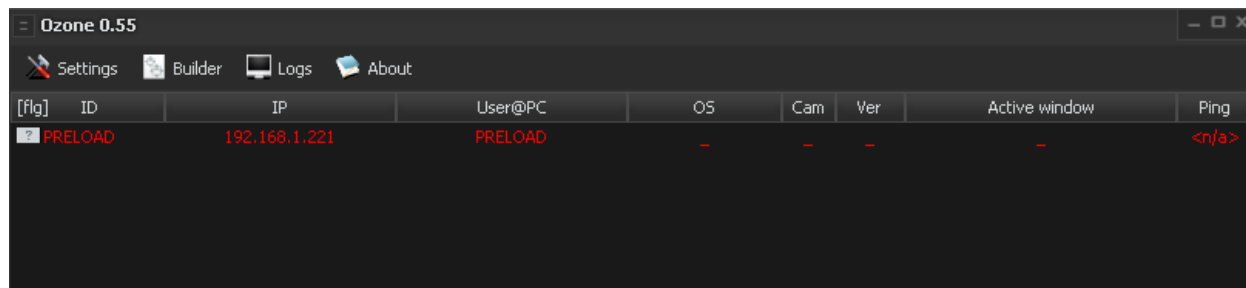
The protocol is characterized by a six byte packet that serves as both a preamble and keep alive. The following is an example of the victim-controller handshake observed during testing:

 Follow TCP Stream (tcp.stream eq 0)

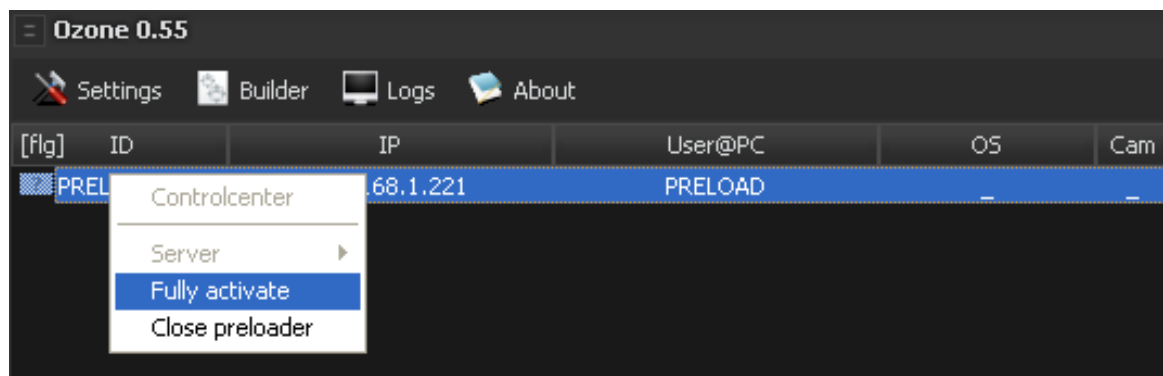


The Ozone handshake “preloads” the victim machine with the control panel:



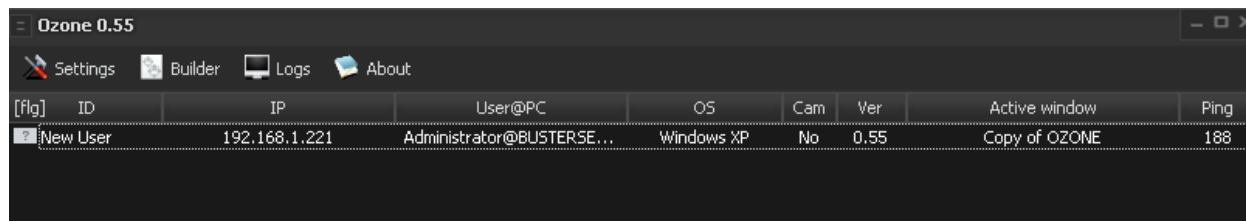


The attacker can then send a command to “fully activate” or “close preloader”:

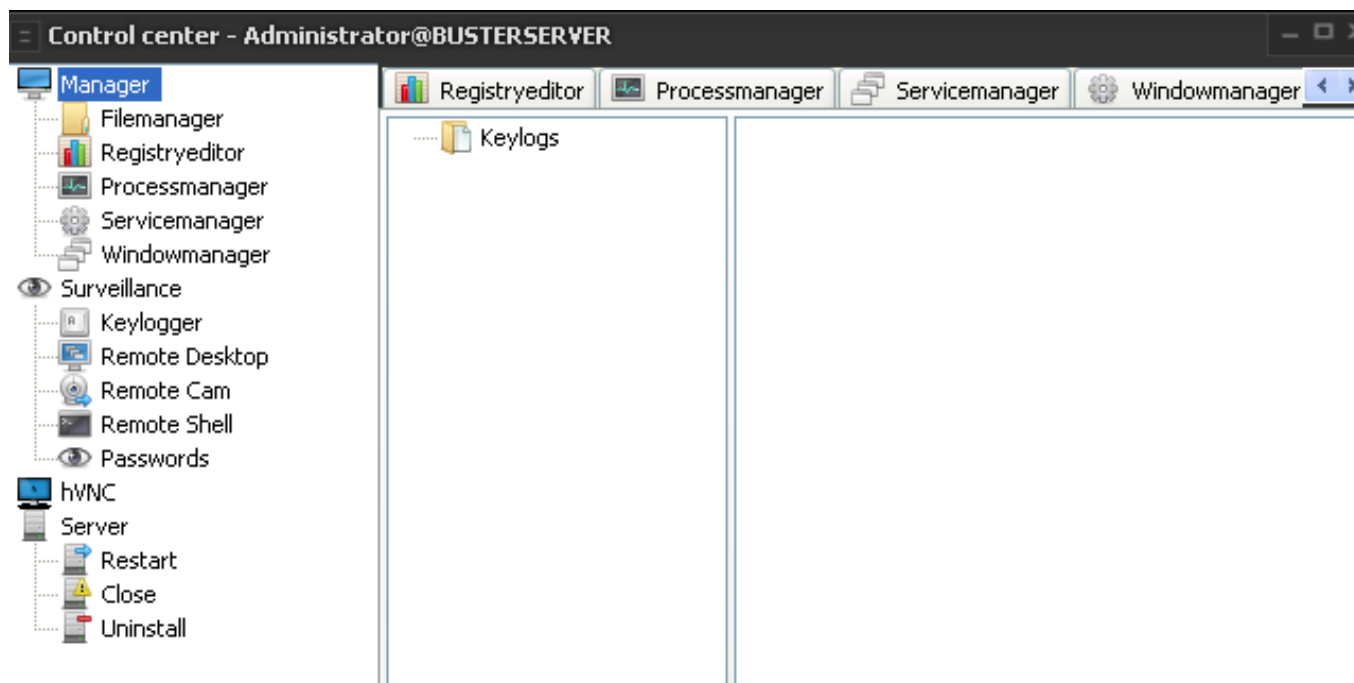


The victim machine is now “fully activated” and all capabilities are functional:





[Flag]	ID	IP	User@PC	OS	Cam	Ver	Active window	Ping
■	New User	192.168.1.221	Administrator@BUSTERSE...	Windows XP	No	0.55	Copy of OZONE	188



The following are recent hashes for Ozone RAT:

```
12f015a9862fd4ebb4d2bcb6b78d1f88865184c833471f2d4d73f17369e64b47
089d270a09c252cbb231d0387d1cef0d958ed521f963d634b6dba75477f72033
86d1420b6dfb6bcc00c9b321cdc164ac18bbcb440a5aa936e0ba8ed63281389b
eb7c969c2a81b133ee4251c0c517e453cd0dcdb7f59ae1b2918ed08a874585e6
e687675c4d557a8b983a558b5d1978fc4021fab565cfe55c5f6ba4d5b7978321
b2b9a95c85b72c8f3756584697ab7fac8679006870a47338345d6b6a67811fa4
86574bce879107dcd15d34c218d2924e9c3b9731ceee9c02d818a6e80c6cfcaa
c5ab02fc9ec73c8348750406b8db6d8fb2af75118ef5de740bf49d125c45649b
b11e98fb5bafb2196a257ce868c70af7edf412ba56128401ec8d2d415dd3ca5e
c083aa18df63700ee2e9fae247d9cb772c049ae9cbf1dde96b60c1a7501d954e
d59bfd5b0046aeeb3e8271d8d98a3cccc48ccb248d7828b23df79ecc90be49d7
```



2374adf01b1aaba43549bc805024a4bf26e2e4b24f819d9ff505d07ef0b7cf04
ca43407ca36f765f96eafb8192e7f2531e53cfc17a71edbd9ae925dd2e8f6373
341022bcd58fec1c7cb2ee2e5e929067ff547f771ef06ee17c54717c62fc49f9
daf72101d9b3ce7c0eaedfeec4ee64e301b7592ce6bec3d203766a26bd45e6e6
8e44de2fbbdb78173647ae1c19a89d1f10ad12ff545bf94329f4cd188172ae55
69fb7eb03010898d460c37461a7b2b0caa5f54d217df9f2d9d32debfe06413e2
32b0b8296a0ab43842b2cad463a32f31a3dec31407237c6cf3a65b925fe1cfd
426ce882b3acf32422d16ff2bd7b296dcd0afc1654f96e0a757ef1462bfd8170
c3efe9510d24b5a233f4f0475839037e9fd7d081ae94ecc083ad1485e5d1e2e7
437f86b236e1a7f6b035b5bd470ec60a65abd353fbee295e742aa22b9b62af4
d414bfa78f72595fc6e54e5012cf47a46004f08f470a8d910484c59cab5fee2f
cb39315dde774e32c66320bfda6b0f77c37758909f2a11338def44e8fd763828
2d29d2cf8670a31547363d6d4b0f405dabaaa14cb76621beb82cee1d9ec69347
a3ed519d38208ca93788fa4c331929643f45cf7e2c1ed1bf8c6b00d74b2b2a68
4adca0ff26d96efcf06c4ea9c8006925335b7b95c82c560c8d0cc466b25fb404
26226c1da0cbe916a25faf55cd5ea66dc33d7e061fc332774e63eea9680e7b56
23f84b69ddfebb6c2c020712af103593732591a1ff506e53bc8ed0044dcbe49e
f755ee5b7e4607da008907cd4fab53bbc652eba397b94a727874c97cbae6d7ff

Recent C2 indicators:

yszforfun.ddns.net
yrzforfun.ddns.net
webearting.duckdns.org
vnc.gamingilluminati.com
steamsupportgroup.no-ip.org
stayhigh.chickenkiller.com
serverupdates.ddns.net
pinballmanager.duckdns.org
microsoftcorporation.duckdns.org
maxboss.noip.me
local.globalnet.ba
keviniscool.dynamic-dns.net
enbo.ddns.net
donut.no-ip.info
dapry428.duckdns.org
dapry428.duckdns.org
breysdass.duckdns.org
applesauce69yolo123.dynamic-
dns.net
antivirus.ddns.net



Mitigations:

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"Ozone Rat checkin";  
flow:established,to_server; dsize:6; content:"|01|"; offset:0;  
content:"|00 00 00 a1|"; offset:2; depth:4; sid:1; rev:1;)
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"Ozone Rat checkin  
blank"; flow:established,to_server; dsize:6; content:"|01 00 00 00 00  
ff|"; offset:0; depth:6; sid:2; rev:1;)
```

rule Ozone

```
{  
meta:  
description = "Ozone Rat - memory strings"  
author = "Mike Murray (MMurray@redskyalliance.org)"  
strings:  
  
$s1 = "SOFTWARE\\Borland\\Delphi\\RTL"  
$s2 = "WinSock 2.0"  
$s3 = "bytes: "  
$s4 = "data.dbf"  
$s5 = "SysUtils"  
$s6 = "m/d/yy"  
$s7 = "$ (,048<@DHLLPPTTXX\\\\"`ddhllppttttxxxx|)|)"  
$s8 = "Running"  
$s9 = "CDATA"  
  
condition:  
all of them  
}
```

