Blog

antivirus SEARCH

Filter: Search Results for "antivirus" - Clear Filter

Newsletter Twitter LinkedIn Discord

Topics

Antivirus Event Analysis Cheat Sheet v1.13.0

by Florian Roth | Jul 17, 2024

We've updated our Antivirus Event Analysis Cheat Sheet to version 1.13.0. It includes updates in several sections New signatures various shell code detections New extensions: .MSC, .VBE, .WLL, .XLL You can download the new version here. Tip: to always find the newest...

Read More

Antivirus Event Analysis Cheat Sheet v1.10.0

by Florian Roth | Aug 13, 2022

We've updated our Antivirus Event Analysis Cheat Sheet to version 1.10.0. It includes updates in several sections add special identifiers for Sliver and Brute Ratel C4 framework implants many new tags for Virustotal assessments You can download the new version here....

Read More

Antivirus Event Analysis Cheat Sheet v1.8

by Florian Roth | Mar 25, 2021

Download the Antivirus Event Analysis Cheat Sheet version 1.8.1 here.

Read More

Antivirus Event Analysis Cheat Sheet v1.4

by Florian Roth | Sep 8, 2018

Download the newest version of our Antivirus Event Analysis Cheat Sheet here. --- Update 09.09.18 10:30am CET Thanks to Markus Neis, I've updated version 1.4 and created a version 1.5 just a few hours after my tweet. You can download version 1.5 here.

Read More

Antivirus Event Analysis Cheat Sheet v1.12.0

by Florian Roth | Jan 20, 2023

We've updated our Antivirus Event Analysis Cheat Sheet to version 1.12.0. It includes updates in several sections New signatures for PUA like FRP and Adfind Signature strings have been sorted alphabetically (not shown in the screenshot below) You can download the new...

Read More

Antivirus Event Analysis Cheat Sheet v1.9.0

by Florian Roth | Feb 6, 2022

We've updated our Antivirus Event Analysis Cheat Sheet to version 1.9.0. It includes updates in almost all sections add special indicators for all kinds of Microsoft Exchange exploitation activity (ProxyLogon, ProxyShell etc.) moves Ransomware indicators to highly...

Read More

Antivirus Event Analysis Cheat Sheet v1.7.2

by Florian Roth | Oct 4, 2019

We've just released an updated version of our Antivirus Event Analysis cheat sheet. You can download version 1.7.2 here. The major changes are: Updated AV signature lists Extended file extension list

Read More

New Antivirus Event Analysis Cheat Sheet Version 1.2

by Florian Roth | May 12, 2018

Today we release a new version of our "Antivirus Event Analysis" Cheat Sheet that helps you with the analysis of Antivirus events by providing a clear decision matrix. We've updated many of the sections, added new VirusTotal online analysis checks and brought it in a...

Read More

Antivirus Event Analysis Cheat Sheet v1.11.0

by Florian Roth | Jan 13, 2023

We've updated our Antivirus Event Analysis Cheat Sheet to version 1.11.0. It includes updates in several sections add special identifiers for other hack tools and ransomware (sync with Sigma rule changes provided by Arnim Rupp in PR #3919 and #3924) You can download...

Read More

Antivirus Event Analysis Cheat Sheet v1.8.2

by Florian Roth | Aug 16, 2021

The analysis of Antivirus events can be a tedious task in big organizations with hundreds of events per day. Usually security teams fall back to a mode of operation in which they only analyze events in which a cleanup process has failed or something went wrong. This...

Read More

Antivirus Event Analysis Cheat Sheet v1.7

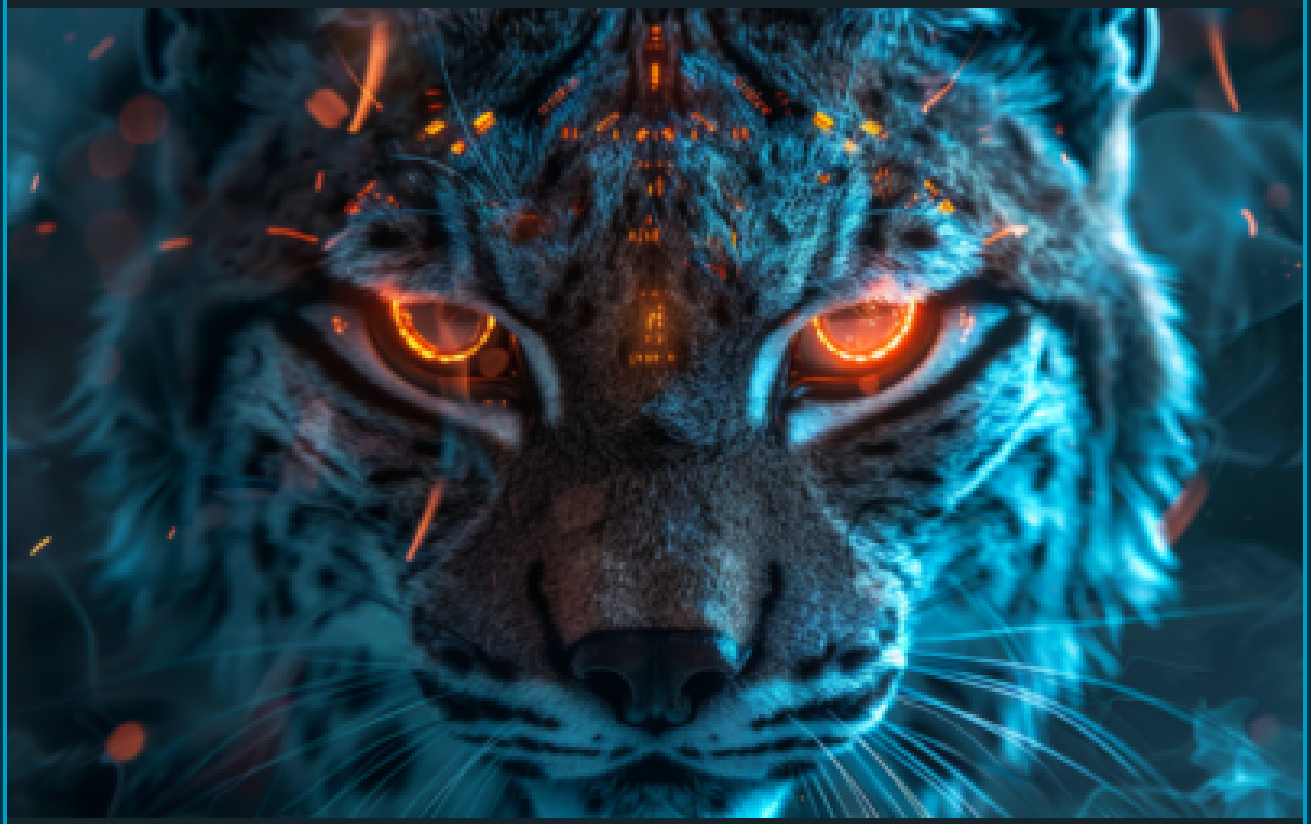
by Florian Roth | Feb 6, 2019

We've just released an updated version of our Antivirus Event Analysis cheat sheet. You can download version 1.7 here.The major changes are:Updated AV signature listsSplit AV signature cells into two columns to save spaceFixed and added some directory namesExtended...

Read More

In-Depth Analysis of Lynx Ransomware

by Nextron Threat Research Team | Oct 11, 2024



Introduction Lynx ransomware is a newly emerged and sophisticated malware threat that has been active since mid-2024. Lynx ransomware has claimed over 20 victims across a range of industries. Once it infiltrates a system, it encrypts critical files, appending a...

Read More

« Older Entries

Resources

Manuals

Fact Sheets

Customer Portal

Company

About Us / Contact

Jobs

Newsletter

Monthly news, tips and insights.

SUBSCRIBE