deep analysis of Xiangoop Loader and EntryShell payload

Targeted attacks using secure USB

VB2023 paper: Targeted attacks using secure USB

Tales from a cloud CSIRT - let’s deep dive into a Kubernetes (k8s) infection

VB2023 paper: Tales from a cloud CSIRT - let’s deep dive into a Kubernetes (k8s) infection

RedStinger: new APT discovered amid Russia-Ukraine conflict

VB2023 paper: RedStinger: new APT discovered amid Russia-Ukraine conflict

The evolution of TA551

VB2023 paper: The evolution of TA551

Let's go door with KCP

VB2023 paper: Let's go door with KCP

Supply chain attack targeting South Asian government delivers Shadowpad

VB2023 paper: Supply chain attack targeting South Asian government delivers Shadowpad

Abusing Electron-based applications in targeted attacks

VB2023 paper: Abusing Electron-based applications in targeted attacks

Darkbit decoded: analysis of an Iranian-sponsored attack

VB2023 paper: Darkbit decoded: analysis of an Iranian-sponsored attack

Lazarus campaigns and backdoors in 2022-2023

VB2023 paper: Lazarus campaigns and backdoors in 2022-2023

Sheep’s clothing of deep & dark web operators: there are no secrets you can hide forever

VB2023 paper: Sheep’s clothing of deep & dark web operators: there are no secrets you can hide forever

Side loading is not dead: the Chinese and the Korean way

VB2023 paper: Side loading is not dead: the Chinese and the Korean way

South Korean Android banking menace - FakeCalls

VB2023 paper: South Korean Android banking menace - FakeCalls

The history and tactics of visa-centric scams in search, spam, and social apps

VB2023 paper: The history and tactics of visa-centric scams in search, spam, and social apps

Terror in Peru: the Zanubis banking trojan

VB2023 paper: Terror in Peru: the Zanubis banking trojan

Looking into TUT’s tomb: the universe of threats in LATAM

VB2023 paper: Looking into TUT’s tomb: the universe of threats in LATAM

Mac-ing sense of the 3CX supply chain attack: analysis of the macOS payloads

VB2023 paper: Mac-ing sense of the 3CX supply chain attack: analysis of the macOS payloads

Don’t flatteN yourself: deobfuscating malware with Control-Flow Flattening

VB2023 paper: Don’t flatteN yourself: deobfuscating malware with Control-Flow Flattening

When a botnet cries: detecting botnets infection chains

VB2023 paper: When a botnet cries: detecting botnets infection chains

Look out! Outlook’s gonna get you!

VB2023 paper: Look out! Outlook’s gonna get you!

"Undocumented"[2:] MSI format. Take it. We are gganbu, aren't we?

VB2023 paper: "Undocumented"[2:] MSI format. Take it. We are gganbu, aren't we?

R2R stomping - are you ready to run?

VB2023 paper: R2R stomping - are you ready to run?

Stolen cookies, stolen identity: how malware makers are exploiting the insecurity of browser data storage

VB2023 paper: Stolen cookies, stolen identity: how malware makers are exploiting the insecurity of browser data storage

May the Shadow Force with Maggie – Shadow Force Group characteristics and relationship to Maggie

VB2023 paper: May the Shadow Force be with Maggie – Shadow Force Group characteristics and relationship to Maggie

Dancing the night away with named pipes

VB2023 paper: Dancing the night away with named pipes

Ransoming and clipping for illicit cryptocurrency gains

VB2023 paper: Ransoming and clipping for illicit cryptocurrency gains

Into the Cumulus: Scarcruft bolsters arsenal for targeting individual Android devices

VB2023 paper: Into the Cumulus: Scarcruft bolsters arsenal for targeting individual Android devices

Intent-based approach to detect email account compromise

VB2023 paper: Intent-based approach to detect email account compromise

How to develop MoleRats defensive strategies: hunt, counterattack and adversary simulation

VB2023 paper: How to develop MoleRats defensive strategies: hunt, counterattack and adversary simulation

Generic script emulation

VB2023 paper: Generic script emulation

Building a cybersecurity AI dataset for a secure digital society

VB2023 paper: Building a cybersecurity AI dataset for a secure digital society

The Dragon who sold his Camaro: reversing a custom router implant

VB2023 paper: The Dragon who sold his Camaro: reversing a custom router implant

C2F2: a framework for detecting C2 frameworks at scale

VB2023 paper: C2F2: a framework for detecting C2 frameworks at scale

MEGALO-(414E)-DON: uncovering data espionage, blackmailing and shell companies in mobile lending apps

VB2023 paper: MEGALO-(414E)-DON: uncovering data espionage, blackmailing and shell companies in mobile lending apps

Teasing the secrets from threat actors: malware configuration extractors

VB2023 paper: Teasing the secrets from threat actors: malware configuration extractors

Web3 will bite you in the Web 2.0: exploring IPFS threats

VB2023 paper: Web3 will bite you in the Web 2.0: exploring IPFS threats

The Dropping Elephant never dropped

VB2023 paper: The Dropping Elephant never dropped

Corporate users in the crosshairs as malvertising gains momentum again

VB2023 paper: Corporate users in the crosshairs as malvertising gains momentum again

SharpTongue: pwning your foreign policy, one interview request at a time

VB2023 paper: SharpTongue: pwning your foreign policy, one interview request at a time

DNS "takeover": the full journey and redemption

VB2023 paper: DNS "takeover": the full journey and redemption

Infostealers: investigate the cybercrime threat in its ecosystem

VB2023 paper: Infostealers: investigate the cybercrime threat in its ecosystem

The rise of China-based financially motivated threat actors?

VB2023 paper: The rise of China-based financially motivated threat actors?

TIPS: Exploring the efficacy of community-driven TI: a real-world approach

VB2023 TIPS presentation: Exploring the efficacy of community-driven TI: a real-world approach

TIPS: Little crumbs can lead to giants

VB2023 TIPS presentation: Little crumbs can lead to giants

TIPS: All for value and value for all – 'Responding RFIs: the merit lies in the difficulty'

VB2023 TIPS presentation: All for value and value for all – 'Responding RFIs: the merit lies in the difficulty'

TIPS: Why joining forces can help solve the crime… or not

VB2023 TIPS presentation: Why joining forces can help solve the crime… or not

TIPS: Dream on: exploring the community effect in cybersecurity

VB2023 TIPS presentation: Dream on: exploring the community effect in cybersecurity

TIPS: AI-based digital evidence enhancement technology for profiling attack groups and techniques to respond to cybersecurity threats

VB2023 TIPS presentation: AI-based digital evidence enhancement technology for profiling attack groups and techniques to respond to cybersecurity threats

TIPS: The global state of scams 2023

VB2023 TIPS presentation: The global state of scams 2023

TIPS: Securing the future: the vital role of computer security vendors in an AI-driven world

VB2023 TIPS presentation: Securing the future: the vital role of computer security vendors in an AI-driven world

TIPS: Emotet in 2023: a comprehensive overview for decision makers on the resurgence, evolution and threat landscape

VB2023 TIPS presentation: Emotet in 2023: a comprehensive overview for decision makers on the resurgence, evolution and threat landscape

TIPS: Operation Cookiemonster – the law enforcement response to the notorious Genesis Market

VB2023 TIPS presentation: Operation Cookiemonster – the law enforcement response to the notorious Genesis Market

Deobfuscating virtualized malware using Hex-Rays decompiler

VB2023 paper: Deobfuscating virtualized malware using Hex-Rays decompiler

Workshop: Modern threat hunting

VB2023 workshop led by VirusTotal

Applied one-to-many code similarity analysis using MCRIT

VB2023 presentation: Applied one-to-many code similarity analysis using MCRIT

Keynote address: Solving cyber insecurity

VB2023 keynote: Solving cyber insecurity

TIPS: Evolution vs extinction & the 10th man

VB2023 TIPS presentation: Evolution vs extinction & the 10th man

Data mining, darknet and chat monitoring - a deep dive into Telegram monitoring and the latest features of the AIL framework

VB2023 presentation: Data mining, darknet and chat monitoring - a deep dive into Telegram monitoring and the latest features of the AIL framework

Keynote: The physics of information asymmetry

VB2023 keynote: The Physics of Information Asymmetry

Turla and Sandworm come filelessly

VB2023 paper: Turla and Sandworm come filelessly

W3LL phishing kit - the tools, the criminal ecosystem, and the market impact

VB2023 paper: W3LL phishing kit - the tools, the criminal ecosystem, and the market impact

Unravelling the MOVEit vulnerability: a journey from exploitation to Clop ransomware infestation

VB2023 paper: Unravelling the MOVEit vulnerability: a journey from exploitation to Clop ransomware infestation

Everything happens for a reason: the choices made by ransomware operators

VB2023 paper: Everything happens for a reason: the choices made by ransomware operators

Hit the bullseye: detecting browser exploits abusing the X memory in WebAssembly

VB2023 paper: Hit the bullseye: detecting browser exploits abusing the X memory in WebAssembly

Browser extensions as an emerging threat vector: unveiling the MANGO malware

VB2023 presentation: Browser extensions as an emerging threat vector: unveiling the MANGO malware

FirePeony: a ghost wandering around the Royal Road

VB2023 paper: FirePeony: a ghost wandering around the Royal Road

$100 hardware backdoors – your old routers may be happily spilling corporate secrets

VB2023 paper: $100 hardware backdoors – your old routers may be happily spilling corporate secrets

USB flows in the Great River: classic tradecraft is still alive

VB2023 paper: USB flows in the Great River: classic tradecraft is still alive

Unveiling activities of Tropic Trooper 2023: deep analysis of Xiangoop Loader and EntryShell payload

VB20203 paper: Unveiling activities of Tropic Trooper 2023: deep analysis of Xiangoop Loader and EntryShell payload

It all makes sense if you don't think about it - misinformation in malware analysis

VB2023 presentation: It all makes sense if you don't think about it - misinformation in malware analysis

Reinventing the steal: Arid Viper now with a Rusty flavour

VB2023 paper: Reinventing the steal: Arid Viper now with a Rusty flavour

Partner presentation: Reversing Nim binaries

VB2023 partner presentation: Reversing Nim binaries

Magniber's missteps: because even spiders trip over their own web

VB2023 paper: Magniber's missteps: because even spiders trip over their own web

Silent whispers of malware: unveiling hidden threats in legitimate network traffic

VB2023 paper: Silent whispers of malware: unveiling hidden threats in legitimate network traffic

Addressing the ransomware threat from outside the lab

VB2023 panel discussion: Addressing the ransomware threat from outside the lab

---