SDC 18
September 24-27, 2018
Santa Clara, CA
www.storagedeveloper.org

Mitigating Evolving Ransomware Attacks at the Block Level with OpenZFS

Michael Dexter
Member, SNIA DPCO

Data Protection and Capacity Optimization Committee

The Reality of Ransomware

"Shadowy bandits have hijacked the PGA America's computer servers, locking officials out of crucial files related to this week's PGA Championship at Bellerive Country Club and the upcoming Ryder Cup in France."

Golfweek, August 8th, 2018

https://golfweek.com/2018/08/08/hackers-target-pga-servers-seek-bitcoin-ransom/

The Reality of Ransomware (Cont.)

High-tech solutions to
low-tech threats

Behavioral Threats

The Reality of Ransomware (Cont.)

No hacking. No “zero days”.

Only users causing harm with existing credentials and permissions

The Reality of Ransomware (Cont.)

Users accidentally encrypting all data they can access is indistinguishable from them *deleting* that data

The response is largely similar

The Reality of Ransomware (Cont.)

The same goes for unauthorized user *exfiltration* of data

The response is largely similar

What is Ransomware?

- SNIA Definition: A type of malicious software (malware) that prevents or limits users from accessing their system, applications, or data, or alternatively, to publish the user's data unless a "ransom" fee is paid
- CryptoLocker, CryptoWall, WannaCry, Petya, StorageCrypter

What is Ransomware? (Cont.)

- Often the unauthorized encryption of data
- Sometimes the unauthorized publication of data
- Ransom payment often by Bitcoin, Premium SMS
- Primarily obtained through “Phishing”
- Often spread by malicious advertising networks

“You won’t believe…”

Ransomware Reach

- Popular file types (.doc(x), .xls(x), .pdf, etc.)
- Network shares
- Online backups
- Document previous versions/“Shadow Copies”
- Cloud accounts and backups, “DropBox”

Anything within reach

Universal Vector: Write Access

- Nefarious in its simplicity
- Indistinguishable from data deletion by users
- Indistinguishable from data exfiltration by users
- Behavioral detection cat and mouse
- Exfiltration is simply unauthorized copy & delete

What is *Evolving* Ransomware

- Branching out from attractive links
- Incorporation of “social engineering” attacks
- Incorporation actual system vulnerabilities (“StorageCrypter” delivered via a Samba issue)
- Potential involvement of state actors

Ransomware Warning Signs

- Out-of-space error as encrypted data replaces unencrypted data
- High write activity from encryption activity
- Actual encryption activity via tracing
- Unusual data exfiltration seen at the firewall

"Suspicious activity" is highly subjective

Ransomware Reality

- Remember that write-access is the risk
- Today's activities can be easily masked tomorrow
- Users and institutions are often silent
- If your users can be tricked, you are at risk

It is impractical to confirm every destructive act such as every save

We regularly escalate privileges

- ‘sudo’ or ‘doas’ on Unix systems
- Windows User Account Control pop-up window
- macOS password request

Escalation would have to be the default behavior

(And your users may rebel)

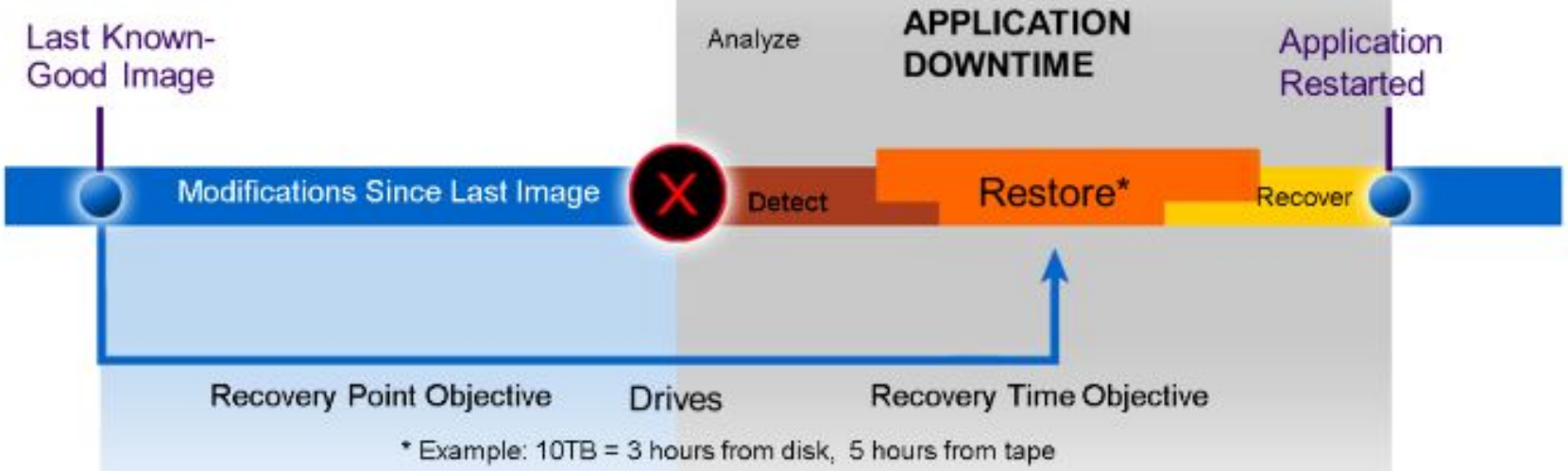
Block-Level Versioning via Snapshotting

- Mitigation must be transparent to the user
  - Outside the reach of user permissions
  - Preferably with a non-destructive undo
  - Preferably at a per-user level
- Requires a clear, coordinated RPO/RTO

Block-Level Versioning via Snapshotting (Cont.)

- RPO: Recovery Point Objective
  - Your acceptable undo window or delta
- RTO: Recovery Time Objective
  - “Help! I lost all my data and my talk’s next!
  - Clear SLA (formal or informal) and *procedures* with users (In case of emergency…)

Recovery Point/Recovery Time Objectives



Block-Level Versioning via Snapshotting (Cont.)

- Many benefits beyond Ransomware mitigation
- Ransomware is the motivator of the hour
- Proactive data protection, not reactive!
- *Assumption of snapshotting abilities in your FS*

Snapshotting File Systems

- FreeBSD UFS2
- GNU/Linux LVM
- Dragonfly BSD HammerFS
- GNU/Linux Btrfs
- NTFS Volume Snapshot Service/Shadow Copies
- WAFL and Oracle ZFS and OpenZFS

Snapshotting File Systems (Cont.)

- Often bolted-on functionality
- Often with performance impacts
- Often with number of snapshots limitations

With the exception of ZFS/OpenZFS

Advanced Snapshotting: OpenZFS

- Copy-On-Write (COW) File System
- Write and dereference, rather than overwrite
- Organized by sequential Transaction Groups
- New data is written as deltas of snapshotted data
- Limited only by hardware limitations

Advanced Snapshotting: OpenZFS (Cont.)

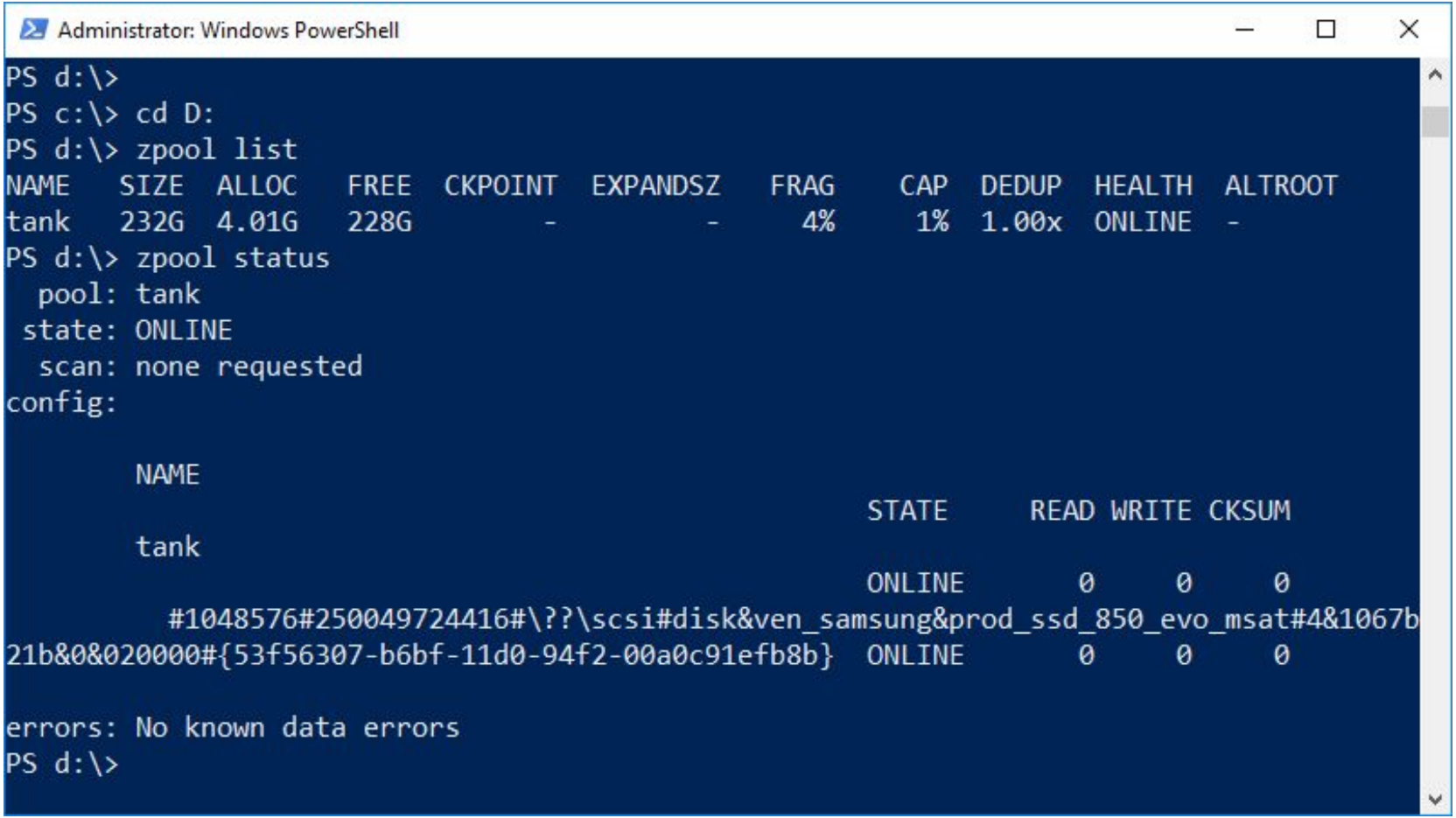
- Fine-grained at the dataset “File System” level
- Writable snapshots in the form of Clones
- Clones allow for forensic preservation
- Promotable to independent File Systems
- Serves as the foundation of OpenZFS replication

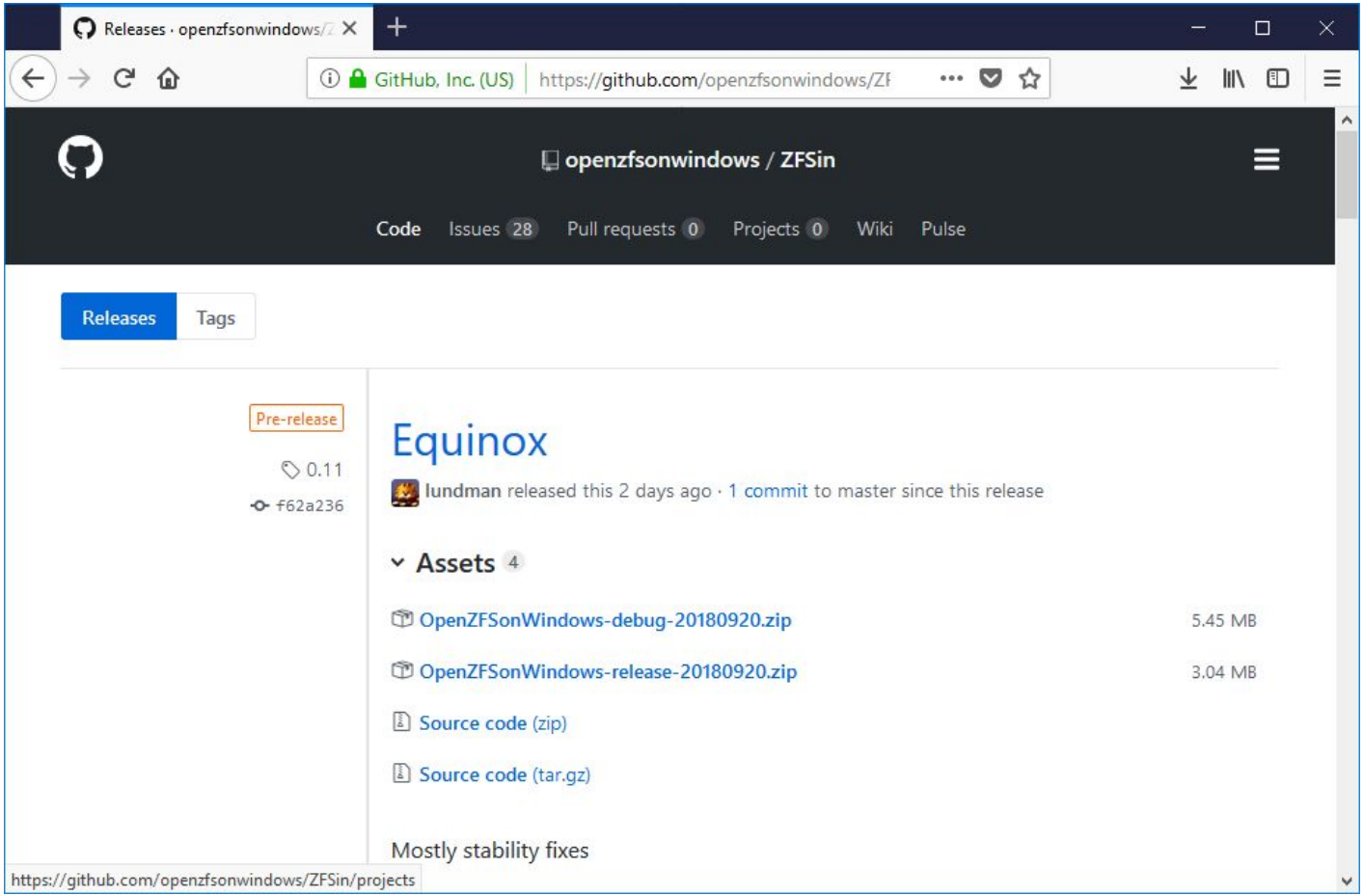
Other OpenZFS Features

- Open Source (Sun CDDL) and **Vendor Neutral**
- Advanced checksumming
- Flexible record (block) sizes and quotas
- “ZVOL” synthetic block devices
  - iSCSI/FC sharing and Virtual Machines
- Supports “hybrid” flash read/write acceleration
- Cross platform/endian-agnostic

OpenZFS in Practice: Operating Systems

- OpenSolaris/Illumos and derivatives
- FreeBSD and derivatives
- GNU/Linux with legal uncertainty
- macOS
- NetBSD (in active development)
- Windows (in active development)





OpenZFS for Developers

- Mature, professional, and welcoming community
- Used by over a dozen NAS projects/products
- Unix/POSIX-oriented but supports “native” object storage (See: Lustre on OpenZFS)
- Fascinating opportunities on Windows

OpenZFS in Practice

- Local File System
- Network File Sharing
  - SMB, NFS, AFP, FTP etc.
- Local or Network block sharing
  - iSCSI, FibreChannel
  - Virtual Machine block devices
  - Brings snapshotting to foreign File Systems!

File and Block: Herein Lies the Flexibility

- “Unified” file and block storage foundation
- Provides rollback to block, file and object storage
- Can mitigate unclean Virtual Machine shutdowns
- Flexible cloning of “golden master” virtual machines
- Can back VMware snapshots and Windows “Shadow Copies”

OpenZFS at the Command Line

```
zfs snapshot myvol/users@2018-09-26
zfs list -t snapshot

NAME                        USED  AVAIL  REFER  MOUNTPOINT
myvol/users@2018-09-26         0      -   780K           -

zfs rollback myvol/users@2018-09-26
```

or

```
zfs clone myvol/users@2018-09-26 myvol/users@recover
```

But, Policy Should Drive Your Technology

- Technical flexibility enables policy flexibility
- Talk to your users about their work habits
- Talk to your lawyers about retention obligations

Ransomware is a Wake Up Call
For Many Perennial Issues

Policy Considerations

- Consciously decide to use snapshots (many don't!)
- Determine when to Snapshot
  - Daily? Hourly? Every five minutes?
  - Running out of space is resolvable but losing historic granularity is *not*
  - During business hours?
  - Usage-driven (MB/GB written)?

Think About Your RPO and Retention

- Your RPO drives your snapshot frequency
- What is your retention policy?
  - The Long Holiday problem
  - “Backup” goals
  - Archiving legal obligations
  - Primary, secondary, tertiary storage?

Mitigating Ransomware In Practice

- My Experience is with FreeBSD and FreeNAS
- Open Source solutions are supportable solutions
- Broad user base with 10M+ FreeNAS downloads
- Culture of vendor and individual contribution
- Excellent overlap with SNIA activities

Regardless of the Platform You Choose…

- Establish and maintain redundancy
  - Flexible and scalable RaidZ/stripe of mirrors
- Create Datasets based on policy/org chart
- Create ZVOL block devices for foreign FSs
- Determine a snapshot and retention policy

Regardless of the Platform You Choose… (Cont.)

- Periodic “scrubs” validate all data checksums
- Replaced failed storage devices as needed
- Watch device S.M.A.R.T.* data
- Determine expected performance
- Recognize degraded performance

*Self-Monitoring, Analysis and Reporting Technology

Emergency Response Procedures

- Communication comes first!
  - Shortens Recovery Time
  - Stops the spread of the Ransomware
  - Helps prevents future infection
- Educate users avoid Ransomware
- Educate users recognize any attack

Emergency Response Procedures (Cont.)

- Infected systems will re-infect – cleanse them
- Clearly communicate what data is impacted
- Decide if forensic information is desirable
- Value metadata as much as data
  - (Company saved by offline AD server in Africa)

Emergency Response Procedures (Cont.)

- Invest in technology and education, not ransoms
- Establish Data Protection policy *before* deployment
- Evolve with the evolving threats
- Learn from every experience and *document it!*

Thank you!

@MichaelDexter
dexter@gainframe.com

Member, SNIA DPCO

Data Protection and Capacity Optimization Committee